Balancing the interests in the context of data retention (INVODAS)

Ireland

Marie McGonagle and Sharon McLaughlin

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

Yes. The provisions of Directive No. 2006/24/EC were transposed into Irish law by the Communications (Retention of Data) Act 2011. This Act was signed into law by the President on the 26th January 2011.

The primary purpose of the Act is to give effect in Irish law to the Directive. The long title of the Act states that it is:

"An Act to give effect to Directive No. 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, to provide for the retention of and access to certain data for the purposes of the prevention of serious offences, the safeguarding of the security of the State and the saving of human life, to repeal Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, to amend the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and to provide for related matters".

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

As noted above, the provisions of Directive 2006/24/EC have been transposed into Irish law by the Communications (Retention of Data) Act 2011. However, there were significant delays in the transposition process.

Formal Delays in the Legislative Procedure

The transposing legislation, the Communications (Retention of Data) Bill 2009, was presented to Dáil Éireann (the House of Representatives) on 9th July 2009 and was passed by it on 24th February 2010. The Bill then began its passage through Seanad Éireann (the Senate) on 29 April 2010 and was scheduled to complete the final stages there on 5th May 2010. However, other legislation was afforded priority by Parliament and, as a result, the legislative process in respect of the transposing legislation was not completed prior to Parliament's summer recess, which began on 8th July 2010. On 20th September 2010, the Criminal Law Reform Division of the Department of Justice, Equality and Law Reform advised the authors that the 2009 Bill would "complete the legislative process in the upcoming Parliamentary session" and would "be signed into law in the near future."

In October 2009, the then Minister for Justice, Equality and Law Reform (Deputy Dermot Ahern TD) attributed the delay in the introduction of the transposing legislation to the Government's decision to transpose Directive 2006/24/EC by means of primary legislation rather than by means of secondary legislation, as was initially intended (691(2) Dáil Debates 278 (8 October 2009)). Deputy Dermot Ahern TD further attributed the delay in the introduction of the 2009 Bill to extended periods of deliberation with service providers, their representative associations and other interested parties (691(2) Dáil Debates 278 (8 October 2009)).

Legal Challenges

Two distinct legal challenges contributed to the delay in introducing and progressing the transposing legislation. The first was taken by the Irish Government concerning the legitimacy of the Directive itself. The second was taken by Digital Rights Ireland challenging the constitutionality of the existing legislation and the Directive.

1. The case taken to the ECJ by the Irish Government

   On 6th July 2006, the Irish Government filed a challenge to Directive 2006/24/EC with the European Court of Justice (ECJ), arguing that the Directive had not been adopted on an appropriate legal basis. Specifically, Ireland contended that the Directive should not have been adopted on the basis of Article 95 EC "since its 'centre of gravity' does not concern the functioning of the internal market but rather the investigation, detection and prosecution of crime, and that measures of this kind ought therefore to have been adopted on the basis of the articles of the EU Treaty relating to police and judicial cooperation in criminal matters." On the 10th February 2010, the ECJ ruled that Article 95 EC constituted the appropriate legal basis for the introduction of the Directive. [Ireland v European Parliament and Council of the European Union (Case C-301/06), judgment of 10 February 2010. See further below.]

2. The case taken to the Irish High Court by Digital Rights Ireland

   Digital Rights Ireland (DRI), a limited liability company concerned with the promotion and protection of civil and human rights in the ICT environment, challenged the constitutionality of Directive 2006/24/EC and of existing national legislation in the Irish High Court. Specifically, DRI argued that Directive 2006/24/EC was contrary to the Charter of Fundamental Rights (CFR), Articles 7, 8, 11 and 41, and the European Convention on Human Rights (ECHR), Articles 8 and 10. In May 2010, the High Court granted the Plaintiff's request for a referral to the European Court of Justice under Article 267 of the Treaty on the Functioning of the European Union (TFEU). [Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources & Ors [2010] IEHC 221; judgment of 5 May 2010. See further below.]

   [Update August 2013: This case was heard by the ECJ on 9th July 2013. The ECJ sent a set of questions it wanted addressed in Oral Submissions to all parties to the case. The website of McGarr Solicitors, acting for DRI, contains a link to the text of the Irish High Court's referral to the ECJ and to the questions sent by the ECJ to all parties involved in the case. Oral Submissions delivered by DRI to the ECJ are also available.

   For more information, see the following:
   - McGarr Solicitors website (acting for DRI), *Digital Rights Ireland: Oral Submission to the European Court of Justice on the Data Retention Directive,* 14th July 2013 available at http://www.mcgarrsolicitors.ie/2013/07/14/digital-

rights-ireland-v-ireland-and-ors-oral-submission-to-the-european-court-of-justice-data-retention-directive/;

- Irish Human Rights Commission (IHRC), *IHRC welcomes High Court decision to consult EU Court of Justice on Privacy Case*, 27th January 2012 available at http://www.ihrc.ie/newsevents/press/2012/01/27/ihrc-welcomes-high-court-decision-to-consult-eu-co/;
- Karlin Lillington, 'Data privacy battle plays out before European court', *The Irish Times*, 11 July 2013.]

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   N/A

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

- ***If transposition has been accomplished:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   Yes. The text of the Communications (Retention of Data) Act 2011 is available at the following link – http://www.oireachtas.ie/documents/bills28/acts/2011/a311.pdf

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   The Communications (Retention of Data) Act 2011 was signed into law by the President on the 26th January 2011.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

b) whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.

The rules which implemented the Directive are in the form of primary legislation – an Act of the Oireachtas (Parliament).

(a) All of the provisions of the Directive contained in Articles 1-10 are covered by the Act.

(b) Initially the Government indicated that it would transpose the Directive by means of secondary legislation (Regulations) and, to this end, published the draft European Communities (Retention of Data) Regulations 2008. However, there was considerable criticism of and opposition to transposition in this way, as well as to the content of the Regulations. The Data Protection Commissioner, for example, raised objections in a letter to the Department and the industry also had concerns (see Karlin Lillington, 'Customers may foot bill for EU data law', The Irish Times, 7 November 2008). The Government then decided to transpose the Directive via primary legislation. It is common for many EU provisions to be transposed by means of secondary legislation, which merely requires a ministerial regulation (Statutory Instrument) to be signed and placed before the Houses of the Oireachtas without parliamentary debate. However, major provisions are generally transposed by means of primary legislation that is subject to the full rigours of parliamentary debate and scrutiny. For example, Directive 2002/58/EC, which did not make significant changes to the existing Directive 97/66/EC in relation to the retention of traffic data, was transposed by means of a Statutory Instrument (S.I. No.535 of 2003); however, the Data Protection Commissioner exerted pressure on the Department in relation to the validity of its use of regulations to authorise data retention and provisions were eventually introduced into an unrelated Bill and passed in 2005. [See further below and Data Protection Commissioner, Annual Report 2002 page 42; Annual Report 2003 page 13.]

8. Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?

Each of the terms defined in Article 2(2) of Directive 2006/24/EC are defined in section 1(1) of the Communications (Retention of Data) Act 2011. The definitions contained in section 1(1) of the 2011 Act are, for the most part, identical to those contained in Article 2(2) of Directive 2006/24/EC. However, there are very slight differences in the definition of "data", "user" and "unsuccessful call attempt".

The differences in the definitions are as follows:

The term "data" is defined in the 2011 Act as "traffic data or location data and the related data necessary to identify the subscriber or user" as opposed to "traffic data and location data and the related data necessary to identify the subscriber or user" in Directive 2006/24/EC.

The term "user" is defined in the 2011 Act as "a person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service" as opposed to "any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service" in Directive 2006/24/EC. It should be noted in this regard, however, that section 18 of the Interpretation Act 2005 provides that the term "person": "shall be read as importing a body corporate ... or an unincorporated body of persons, as well as an individual ....". In other words, in Irish law, the term "person" includes any legal entity or natural person.

The term "unsuccessful call attempt" is defined in the 2011 Act as "a communication where a telephone call or an Internet telephony call has been successfully connected but not answered or there has been a network management intervention" as opposed to "a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention" in Directive 2006/24/EC.

Additional terms defined in the national legislation:

The term "service provider" is used several times in Directive 2006/24/EC and, while not expressly defined in Article 2(2) of the Directive, it is defined in section 1(1) of the national legislation. The definition is: "a person who is engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet."

In addition to defining the terms contained in Article 2(2) of the Directive, the 2011 Act also defines "designated judge", "disclosure request", "Referee", "revenue offence" and "serious offence" – none of which are defined in the Directive.

Further, section 1(2) of the 2011 Act states: "A word or expression used in this Act and also in Directive 2002/58/EC has the same meaning in this Act as in that Directive."

Definitions in Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC:

The terms defined in Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC are not defined in the Communications (Retention of Data) 2011 Act (aside from the definition of "user", which is defined in the 2011 Act and in Directives 2002/21/EC and 2002/58/EC). However, the majority of definitions

contained in Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC are defined in other national statutes and regulations, namely the Data Protection Act 1988, Communications Regulation Act 2002, Data Protection (Amendment) Act 2003 and the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.

Directive 95/46/EC

Article 2 of Directive 95/46/EC defines "personal data", "processing", "filing system", "controller", "processor", "third party", "recipient" and "data subject's consent."

Nationally, section 1(1) of the Data Protection Act 1988 defines "controller" and "processor." Additionally, section 1(2) of the Data Protection (Amendment) Act 2003, introduced in order to give effect to Directive 95/46/EC, defines "personal data", "processing" and "relevant filing system." The terms "third party", "recipient" and "consent" appear several times in the 2003 Act but are not defined. The term "consent" is however defined in section 2(1) of the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.

Directive 2002/21/EC

Article 2 of Directive 2002/21/EC defines "electronic communications network", "transnational markets", "electronic communications service", "public communications network", "associated facilities", "conditional access system", "national regulatory authority", "user", "consumer", "universal service", "subscriber", "provision of an electronic communications network", "end-user", "enhanced digital television equipment" and "application program interface (API)."

Nationally, section 2(1) of the Communications Regulation Act 2002 defines "electronic communication network", "electronic communications service", "associated facilities", "conditional access system", "user" and "universal service." The term "national regulatory authority" is not defined in the 2002 Act but section 10(4) stipulates that the Commission for Communication Regulation (ComReg) is the designated authority for the purposes of the legislation. In addition, while the phrase "provision of an electronic communications network" appears in the 2002 Act, it is not defined. The terms "end-user", "enhanced digital television equipment, "application program interface (API)", "transnational markets", "public communications network" and "consumer" are not defined in Irish legislation relevant to this area. The term "subscriber" is defined in the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.

Directive 2002/58EC

Article 2 of Directive 2002/58/EC defines "user", "traffic data", "location data", "communication", "call", "consent", "value added service" and "electronic mail". Section 2(1) of the European Communities (Electronic Communications Networks

and Services) (Data Protection and Privacy) Regulations 2003, introduced to give effect to Directive 2002/58/EC, defines all of the terms contained in Article 2 of the Directive.

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

"Data" is defined in section 1(1) of the Communications (Retention of Data) Act 2011 as "traffic data or location data and the related data necessary to identify the subscriber or user."

Part One of Schedule 2 of the 2011 Act specifies the data to be retained by service providers in relation to fixed network and mobile telephony. Service providers must retain data necessary to trace and identify the source of a communication; to identify the destination of a communication; to identify the date and time of the start and end of a communication; to identify the type of communication; to identify users' communication equipment or what purports to be their equipment; and to identify the location of mobile communication equipment (mobile telephony only).

Part One of Schedule 2 of the 2011 Act reflects exactly the provisions contained in Article 5 of the Directive in relation to the categories of data to be retained in respect of fixed line and mobile telephony.

Part Two of Schedule 2 of the 2011 Act specifies the data to be retained by service providers in relation to Internet access, Internet email and Internet telephony. Service providers must retain data necessary to trace and identify the source of a communication; to identify the destination of a communication; to identify the date, time and duration of a communication; to identify the type of communication; and to identify users' communication equipment or what purports to be their equipment.

Part Two of Schedule 2 of the transposing legislation reflects exactly the provisions contained in Article 5 of the Directive in relation to the categories of data to be retained in respect of Internet access, Internet e-mail and Internet telephony.

Section 3(4) of the 2011 Act provides that the data required to be retained include data relating to unsuccessful call attempts but that in the case of unsuccessful call attempts the data need to be retained only where, in relation to telephone data, the data are stored in the State and, in relation to Internet data, the data are logged in the State.

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the

content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

As can be seen from the long title to the Communications (Retention of Data) Act 2011 set out in answer to question 1 above, there is other legislation in place in Ireland that provides for data retention. The long title of the 2011 Act expressly refers to Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which was repealed by section 13 of the 2011 Act, was headed "Communications Data". Section 62 made clear that the provisions applied only to telephony data and did not apply to content. Secton 63(1) pertained to traffic or location data or both and s.63(6) specifically excluded aggregated data and data that had been made anonymous. Section 63 replaced ministerial directions (i.e. not legislation) issued in 2002 under the Postal and Telecommunications Services Act 1983 to service providers obliging them to retain data for not less than three years. (See explanatory memorandum to the Criminal Justice (Terrorist Offences) Act 2005, available at: < http://www.oireachtas.ie/documents/bills28/acts/2005/a0205.pdf>).

Part 7 of the 2005 Act continued the three year retention period (s.63(1)).

Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, now repealed by section 13 of the 2011 Act, was added by the Government by way of amendments at a late stage in the passage of the Bill through the Houses of the Oireachtas. (The Bill was the Criminal Justice (Terrorist Offences) Bill 2002, but the amendments adding Part 7 to it were not introduced by the Government until 3 February 2005.) While Part 7 did not specify any particular types or categories of data other than traffic or location data, the lack of clear definition and scope allowed for the possibility of overreach and fishing expeditions. The Data Protection Commissioner, for example, reported that call records had been accessed over 10,000 times in the first eighteen months that Part 7 was in operation. (See 635 Dáil Éireann 761 (4 April 2007); 202(6) Seanad Éireann 405 (29 April 2010); and Karlin Lillington, 'All is not well on the data protection front', The Irish Times, 4 March 2010).

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

Under the terms of the Communications (Retention of Data) Act 2011, data retention is mandated for purposes of: (a) the prevention, detection, investigation or prosecution of a serious offence; (b) the safeguarding of the security of the State; and (c) the saving of human life (see long title to the Act, cited above in answer to question 1, and see also s.6(1) of the Act).

The 2011 Act does not elaborate on what is meant by "security of the State" nor does it elaborate on when the requirement of "saving human life" is satisfied. It should, however, be noted that Directive 2006/24/EC requires telephony and internet service providers to retain data for a specified period for purposes of

detecting, investigating and prosecuting serious crime. The requirement to retain data for the purpose of "saving human life", as contained in the 2011 Act (s.6), is therefore surplus to the requirements of Directive 2006/24/EC.

"Serious offence" is defined in section 1(1) of the 2011 Act as "an offence punishable by imprisonment for a term of 5 years or more, and an offence listed in Schedule 1 is deemed to be a serious offence." Schedule 1 of the 2011 Act lists a number of offences, deemed to be "serious offences" for the purposes of the legislation, triable on indictment but carrying a maximum penalty of less than 5 years. According to the parliamentary deliberations on the 2011 Act, the offences listed in Schedule 1 were suggested by the Garda Síochána (the Irish police force) and "represents its opinion on the offences for which it is essential it retains the ability to make a disclosure request, namely, offences carrying a penalty of up to five years imprisonment" (691(2) Dáil Debates 280 (8 October 2009)). These offences are:

a) An offence under sections 11 and 12 of the Criminal Assets Bureau Act 1996 – section 11 makes it an offence to identify an officer/former officer of the bureau, a member/former member of staff of the bureau, or the fact that an individual is a member of the family of a bureau officer/former officer or member/former member of staff of the bureau and section 12 makes it an offence to delay, obstruct, impede, interfere with or resist a bureau officer in the exercise or performance of his or her powers or duties.

b) An offence under section 6 of the Criminal Evidence Act 1992 – section 6 makes it an offence to make a false statement in a certificate of evidence.

c) An offence under section 12 of the Non-Fatal Offences Against the Person Act 1997 – section 12 deals with the offence of poisoning.

d) An offence under section 1 of the Prevention of Corruption Acts 1889 to 1995 – section one deals with corrupt transactions with agents.

e) An offence under section 5 of the Protections for Persons Reporting Child Abuse Act 1998 – section 5 makes it an offence to make false reports of child abuse.

The 2011 Act (s.6(1)) therefore provides for An Garda Síochána to request a service provider to disclose data retained by the service provider for any of the purposes listed above.

In addition, section 6(2) of the 2011 Act provides for the Permanent Defence Force to request a service provider to disclose data retained by the service provider for the purpose of safeguarding the security of the State and section 6(3) permits the Revenue Commissioners to request a service provider to disclose data retained by the service provider for the purpose of the prevention, detection, investigation or prosecution of a revenue offence (the term "revenue offence" is defined in section 1(1) of the Act).

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?**

The Communications (Retention of Data) Act 2011 does not contain any provisions in respect of sensitive data as such.

The Data Protection Acts 1988-2003 define "sensitive personal data" as "personal data as to – (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade-union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings."

The Data Protection Acts require additional conditions to be met for the processing of such data to be legitimate. Usually this will be the consent of the person about whom the data relates.

As noted supra, under the Communications (Retention of Data) Act 2011, data retention is mandated for the purpose of the prevention, detection, investigation or prosecution of a serious offence. Under the terms of the Data Protection Acts 1988-2003, data pertaining to "the commission or alleged commission of any offence by the data subject" and "any proceedings for an offence committed or alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings" is deemed to be "sensitive personal data." The 2011 Act, therefore, by its very nature, deals with "sensitive personal data."

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

Under the terms of the Communications (Retention of Data) Act 2011, data in respect of fixed line and mobile telephony must be retained for a period of 2 years and data in respect of Internet access, Internet e-mail and Internet telephony must be retained for a period of 1 year.

Prior to this, the Data Protection Commissioner had revealed that, having made an order in January 2001 requiring telcos and ISPs to register with his office, he discovered that all traffic data for telcos was being routinely retained for a period of six years, i.e. the full period envisaged for bringing claims under the Statute of Limitations Act (see Data Protection Commissioner, Annual Report, 2002, p.41). The Commissioner pressed for a six month period of retention but, in March 2002,

on the basis of concerns regarding access for security and crime investigations, the Government decided that the Minister for Public Enterprise should issue Directions under s.110(1) of the Postal and Telecommunications Services Act 1983 requiring telcos to retain detailed non-anonymous traffic data for a three year period. The Direction was issued in April 2002 and described as a temporary holding measure pending the introduction of substantive legislation (see Data Protection Commissioner, Annual Report, 2002, pp. 41-42). As no such legislation emerged, the Data Protection Commissioner issued enforcement notices to the telecommunications companies in January 2005 requiring them to hold traffic data for national security purposes for a maximum period of twelve months. Two of the companies appealed to the Circuit Court but, on 3 February, the Government amended the Criminal Justice (Terrorist Offences) Act 2005 and the Bill containing the new Part 7 (see above answer to question 10) was subsequently passed. The Commissioner cancelled the enforcement notices on 7 February in the expectation that the Bill would pass by 1 May 2005 (see Data Protection Commissioner, Annual Report, 2004, p.4).

Under Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 – now repealed by section 13 of the Communications (Retention of Data) Act 2011 – telephony data had to be retained for a period of three years. The 2005 Act made no provision regarding the retention of Internet data.

During the course of parliamentary debates on the Communications (Retention of Data) Act 2011, the then Minister for Justice, Equality and Law Reform (Dermot Ahern TD) stated that the requirement to retain telephony data for a period of 2 years contained in the transposing legislation was not a derogation of the 3 year period contained in the 2005 Act. In this regard, the Minister referred to Article 95(4) of the TEC which provides that if, after the adoption of a harmonisation measure, a Member State deems it necessary to maintain national measures, it can notify the Commission of those provisions and the grounds for maintaining them (691(2) Dáil Debates 280-281 (8 October 2009)).

The parliamentary debates relevant to the transposing legislation reveal that the selection of a 2 year retention period in respect of telephony data and a 1 year retention period in respect of Internet data came about as a result of consultations with the Garda Síochána. During this consultation process, the Garda Síochána opined that these retention periods were the minimum periods required for the investigation of serious crime and safeguarding the security of the state (691(2) Dáil Debates 280-281 (8 October 2009)).

14. Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?

Under the terms of the Communications (Retention of Data) Act 2011, a member of the Garda Síochána (the Irish police force) not below the rank of chief superintendent, an officer of the Permanent Defence Forces not below the rank of

colonel and an officer of the Revenue Commissioners not below the rank of principal officer may make a disclosure request (s.6).

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

Under section 6(1) of the 2011 Act, the Garda Síochána (members not below the rank of chief superintendent) may request disclosure of retained data where that member is satisfied the data are required for:

(a) the prevention, detection, investigation or prosecution of a serious offence,

(b) the safeguarding of the security of the State,

(c) the saving of human life.

Section 6(2) states that members of the Permanent Defence Forces (not below the rank of colonel) may request disclosure of retained data where that member is satisfied the data are required for the purpose of safeguarding the security of the state.

Section 6(3) states that the Revenue Commissioners (officers not below the rank of principal officer) may request disclosure of retained data where that member is satisfied the data are required for the prevention, detection, investigation or prosecution of a revenue offence.

See further answer to question 11.

In addition, section 64(2) of the Criminal Justice (Terrorist Offences) Act 2005 – now repealed by section 13 of the Communications (Retention of Data) Act 2011 – permitted the Garda Síochána (members not below the rank of chief superintendent) to request the disclosure of data in the possession of service providers for the purposes of preventing, investigating, detecting or prosecuting crime, including terrorist crime, or safeguarding the security of the State.

In Ireland, the term "serious offence" is defined in the Bail Act 1997 (s.1) as an offence "for which a person of full capacity and not previously convicted may be punished by a term of imprisonment for a term of 5 years or by a more severe penalty." The Schedule to the Bail Act 1997 specifies the offences deemed "serious offences" for the purposes of the Act. The Criminal Justice (Terrorist Offences) Act 2005 (Part 6, s. 60) amends the Schedule to the Bail Act 1997 by extending it to include "any offence under the Criminal Justice (Terrorist Offences) Act 2005."

The Communications (Retention of Data) Act 2011, s.1, defines a "serious offence" as an "offence punishable by imprisonment for a term of 5 years or more, and an

offence listed in Schedule 1 is deemed to be a serious offence." Schedule 1 to the 2011 Act ("Offences Deemed to be Serious Offences") contains a number of offences deemed to be serious offences for the purposes of the Act. The offences contained in Schedule 1 are triable on indictment but carry a maximum penalty of less than five years. The list of offences contained in Schedule 1 "was suggested by the Garda Síochána and represents its opinion on the offences for which it is essential it retains the ability to make a disclosure request, namely, offences carrying a penalty of up to five years imprisonment" (Deputy Dermot Ahern, then Minister for Justice, Equality and Law Reform, 691(2) Dáil Éireann 280 (8 October 2009)).

The Criminal Justice (Terrorist Offences) Act 2005 also permitted the Permanent Defence Forces (members not below the rank of colonel) to request the disclosure of data in the possession of service providers for the purpose of safeguarding the security of the state (s.64(3)).

Section 64 of the 2005 Act – now repealed – also stated that data were to be disclosed by the service provider in accordance with a court order, for the purpose of civil proceedings in any court or as may be authorised by the Data Protection Commissioner (s.64(1)(c)-(e)).

The 2011 Act does not provide for the right of any other individuals to access the data or for any other usage of it.

16. Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?

See answer to question 15.

17. Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?

No. It is not required to obtain a court order before accessing the data retained.

Section 64 of the Criminal Justice (Terrorist Offences) 2005 Act, now repealed by section 13 of the Communications (Retention of Data) Act 2011, stipulated that service providers shall not access data retained in accordance with section 63(5) except "[…] (c) in accordance with a court order, or (d) for the purpose of civil proceedings in any court […]". Section 5 of the 2011 Act states:

1. A service provider shall not access data retained in accordance with *section 3* except — at the request and with the consent of a person to whom the data relate,

2. for the purpose of complying with a disclosure request,

3. in accordance with a court order, or

4. as may be authorised by the Data Protection Commissioner.

In addition, it is worth pointing out that in the case of EMI v. Eircom [2005] 4 IR 148 (which concerned copyright infringement), it was held that, in circumstances where unknown persons have committed a wrongful activity, a court order may be made requiring a defendant (in this case, an ISP) to identify such persons for the purpose of litigation.

Under the Communications (Retention of Data) Act 2011, it is not required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed.

See further answer to question 18.

18. Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?

No. An individual does not have the right under the 2011 Act to be notified that data relating to him/her have been accessed (i.e., have been the subject of a disclosure request).

During the course of parliamentary deliberations on the transposing legislation, it was argued that section 10 (see further answer to question 20) should be amended to provide for a duty of notification of a person in respect of whom data has been requested. Specifically, it was suggested that the individual to whom the data relates should, after a period of time, be notified that his/her data has been the subject of a disclosure request (202(6) Seanad Debates 406 (29 April 2010)).

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

See answer to question 16.

Under the 2011 Act, an individual can only find out if data relating to him or her has been accessed on foot of a disclosure request. Under section 10, a person who believes that his or her data has been the subject of a disclosure request can apply to the Referee for an investigation into the matter.

"It is not a function of the Referee to investigate whether a disclosure request has been made and to inform the applicant accordingly. The role of the Referee is to investigate whether a disclosure request has been made as alleged, and if so, whether the provisions of section 6 have been complied with. In other words, the Referee must investigate whether the disclosure request was made for the purposes set out in that section, that it was made in writing except in cases of exceptional urgency and that administrative procedures were followed. The referee will not inform the applicant if a request has been properly made in accordance with section 6 or if no request has been made. To be obliged to do so would give rise to fishing

expeditions and would have serious consequences for criminal investigations and state security."

(Statement by Peter Power, Communications (Retention of Data) Bill 2009: Committee Stage, 11th November 2009).

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

Section 10(2) of the transposing legislation states:

A person who believes that data that relate to the person and that are in the possession of a service provider have been accessed following a disclosure request may apply to the Referee for an investigation into the matter.

If, having investigated the matter, the Referee decides that there has been a breach of section 6 of the legislation, section 10(4) states that the Referee shall:

(a) notify the applicant in writing of that conclusion, and

(b) make a report of the Referee's findings to the Taoiseach [i.e., Prime Minister].

In addition, section 10(5) of the transposing legislation states that the Referee, in the circumstances specified in section 10(4), may:

(a) direct the Garda Síochána, the Permanent Defence Force or the Revenue Commissioners to destroy the relevant data and any copies of the data,

(b) make a recommendation for the payment to the applicant of such sum by way of compensation as may be specified in the order.

A decision of the Referee is final (s.10(8)).

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

Section 4(1) of the Communications (Retention of Data) Act 2011 states that a service provider who retains data under the Act must take a number of security measures in relation to the data. The measures specified in s.4(1) of the 2011 Act are:

(a) the data shall be of the same quality and subject to the same security and protection as those data relating to the publicly available electronic communications service or to the public communications network, as the case may be;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by authorised personnel only;

(d) the data, except those that have been accessed and preserved, shall be destroyed by the service provider after—

(i) in the case of the data in the categories specified in Part 1 of Schedule 2, a period of 2 years and one month, or

(ii) in the case of the data in the categories specified in Part 2 of Schedule 2, a period of one year and one month.

Section 4(2) designates the Data Protection Commissioner as the national supervisory authority.

Section 5 of the 2011 Act states that service providers shall not access data retained by them except: at the request and with the consent of a person to whom the data relate; for the purpose of complying with a disclosure request; in accordance with a court order; or as may be authorised by the Data Protection Commissioner.

22. When do the accessing bodies have to destroy the data transmitted to them?

As noted above, the Communications (Retention of Data) Act 2011 states that service providers have 1 year and one month to destroy Internet data and 2 years and one month to destroy telephony data (s.4(1)). There is no provision in the transposing legislation requiring the accessing bodies – the Garda Síochána, Permanent Defence Forces and Revenue Commissioners – to destroy Internet and/or telephony data accessed by them within a specified period of time.

The transposing legislation (s.10(5)) states that the Referee may direct the accessing bodies to destroy the data in circumstances where the Referee has deemed there was an infringement of s.6 of the legislation.

The Data Protection Acts 1988-2003 state that data controllers should retain data for no longer than is necessary for the purpose or purposes for which they are kept (s.2).

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

The legislation itself does not specify the actual service providers which are obligated to retain the data. It appears, therefore, that the 2011 Act applies to all service providers who fall within the definition of "service provider" in the Act: "a

person who is engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet" (s.1).

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

No such distinction is made in the transposing legislation.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

The Data Protection Acts 1988-2003 state that data controllers shall keep personal data only for one or more specified and lawful purposes (s.2(1)(c)(i)) and personal data shall not be kept for longer than is necessary for that purpose (s.2(1)(c)(iv))). The term "lawful purpose" is not defined in the 1988 Act; however, the processing of personal data by service providers is a recognised "lawful purpose."

Section 2(1)(c)(i) of the Data Protection Act 1988 provides that data controllers shall obtain personal data only for "one or more specified, explicit and legitimate purposes." Section 2(1)(c)(iv) further provides that personal data shall not be kept "for longer than is necessary for that purpose or those purposes." It is legitimate for telcos and ISPs to process personal data for billing purposes.

Section 2(5) of the 1988 Act deals with the retention of personal data for statistical or research or other scientific purposes, and the keeping of personal data which complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects.

Section 2(7) of the 1988 Act deals with the keeping of personal data for direct marketing purposes.

Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, now repealed by section 13 of the Communications (Retention of Data) Act 2011, related to telephony data (data relating to communications transmitted by means of a fixed line or mobile telephone - s.62), traffic or location data or both but not aggregated data or data that has been made anonymous (s.63). Traffic or location data, when requested by the Garda Commissioner, had to be retained for a period of three years for the purposes of (a) the prevention, detection, investigation or prosecution of crime (including but not limited to terrorist offences), or (b) the safeguarding of the security of the State.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system

stability and reliability, against unauthorised destruction, loss or alteration of the data)?

Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 (s.63(2)) – repealed by section 13 of the Communications (Retention of Data) Act 2011 – provided that the data retention request must be made in writing.

Section 64 of the 2005 Act – now repealed – provided that a service provider shall not access data retained in accordance with section 63(5), except—

(a) at the request and with the consent of the person to whom the data relate,

(b) for the purpose of complying with a disclosure request under subsection (2) or (3) of this section,

(c) in accordance with a court order,

(d) for the purpose of civil proceedings in any court, or

(e) as may be authorised by the Data Protection Commissioner.

It further provided that only senior officers above a stated rank could access the data. A disclosure request had to be made in writing, but in cases of exceptional urgency the request could be made orally (whether by telephone or otherwise) by a person entitled to make the request.

Apart from providing a complaints procedure, s.67 provided for the appointment of a High Court judge to inter alia keep the operation of the provisions of this Part of the Act under review and ascertain whether the Garda Síochána and the Permanent Defence Force are complying with its provisions. The Revenue Commissioners were not an accessing body under the 2005 Act.

Otherwise, Part 7 was silent on the issue of data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data.

27. **Which *additional* costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in *total* from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?**

There are no actual figures available in respect of additional costs. According to Paul Durrant, General Manager of the Internet Service Providers Association of Ireland (ISPAI), additional costs are capable of being broken down as follows:

1. Initial capital costs and labour costs of technical changes, software and equipment necessary to capture the data required by the law.

2. Running and maintenance costs of storage and its backup to hold this additional data.

3. Data Request processing labour costs plus communication and other expenses that may be incurred on each request.

4. Personnel time spent in court as technical witness to substantiate evidence.[1]

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

No. The Communications (Retention of Data) Act 2011 is silent on the issue of costs and does not make provision for reimbursement of costs to service providers.

Concern about the financial burden which will be placed upon service providers by the legislative requirement to retain data in the manner prescribed is a recurring theme throughout the parliamentary deliberations on the 2011 Act. For example, one member of parliament (Sean Sherlock TD) argued that the costs commensurate with retaining Internet and telephony data for the periods specified in the transposing legislation "could be prohibitive and reduce any future comparative advantage Ireland might gain through the Internet and telecommunications sectors" (703(2) Dáil Debates 318 (24 February 2010).

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

Section 6 of the transposing legislation sets out the procedure for the making of disclosure requests in respect of data retained by service providers. Disclosure requests must be made in writing; however, in cases of exceptional urgency, requests may be made orally. Oral requests for disclosure must be confirmed in writing within two working days of the request being made.

Section 7 of the transposing legislation states that:

"A service provider shall comply with a disclosure request made to the service provider."

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

Section 65(4) of the Criminal Justice (Terrorist Offences) Act 2005, now repealed by section 13 of the Communications (Retention of Data) Act 2011, provided that the Complaints Referee, if he found a contravention of the provisions in relation to

[1] The authors received personal email correspondence from Paul Durrant, General Manager of the Internet Service Providers Association of Ireland (ISPAI) on 8th October 2010.

disclosure, could make a recommendation for the payment of compensation to the applicant.

Under section 10 of the Communications (Retention of Data) Act 2011, the Complaints Referee, where he concludes that there has been a breach of proper procedures (section 6), may make a recommendation for the payment of compensation by the Minister for Justice, Equality and Law Reform.

Under section 10 of the 2011 Act, the Referee is empowered to investigate whether a disclosure request contravenes section 6. Section 6 of the 2011 sets out the procedure for making a disclosure request and, as such, relates to the accessing bodies.

Under section 7, service providers are obliged to comply with any disclosure requests made to them and, under section 4, service providers are obliged to delete retained data (except those that have been accessed and preserved) after a specified period of time. Section 10, however, makes no reference to investigating alleged breaches of these obligations.

Where the Complaints Referee makes a recommendation for the payment of compensation to the applicant (section 10(5)(b)), the Minister for Justice, Equality and Law Reform has responsibility for the implementation of this recommendation (section 10(6)).

The State pays the compensation.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

The accessing bodies (see answer to question 14) are responsible for establishing contact with the retaining parties.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

No. The only entities permitted to access data under the terms of the Communications (Retention of Data) Act 2011 are the Garda Síochána (Irish police force), Permanent Defence and Revenue Commissioners (see answer to question 14).

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)?

Have general rules of co-operation been adapted in the course of the Directive's transposition?

It is believed that there are ongoing discussions between the various bodies as to how the system envisaged in the 2011 Act will be operated in practice (see further answer to question 38 below).

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies dispose of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

The transposing legislation does not contain any rules governing the exchange of retained data with other EU Member States, EEA Member States and/or third countries. However, while there is no specific legal basis providing for such exchange, it can be assumed that traditional mutual assistance routes would be available.[2]

The Data Protection (Amendment) Act 2003 implemented EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data within the EEA.

Section 11 of the Data Protection Acts 1988-2003 specify conditions that must be met before personal data may be transferred to third countries. Personal data cannot be transferred to third countries unless the country "ensures an adequate level of data protection" (s.11(1)). If the third country does not provide an adequate level of data protection, the Irish data controller must rely on use of approved contractual provisions or one of the other alternative measures set out in section 11(4). The Irish Data Protection Commissioner retains the power to prohibit transfers of personal data to any country (not just third countries), except in cases where the transfer is required or authorised by law, or where the transfer is required by an international agreement which Ireland is obligated to enforce (s.11(7)).

[2] The authors received email correspondence to this effect from the Office of the Data Protection Commissioner on 11th October 2010.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

Under section 4 of the Communications (Retention of Data) Act 2011, the Data Protection Commissioner is designated as the national supervisory authority for the purposes of the Act. Section 4 of the 2011 Act gives effect to Articles 7 and 9 of Directive 2006/24/EC. The Data Protection Commissioner is appointed by Government and is independent in the exercise of his functions.

Section 9 of the Data Protection Act 1988 established the Office of the Data Protection Commissioner. The Data Protection Commissioner is responsible for investigating alleged contraventions of data protection legislation by data controllers and data processors (section 10, 1988 Act); is empowered, under certain circumstances, to prohibit the transfer of personal data outside the state (section 11, 1988 Act); is empowered to require information (section 12, 1988 Act); is mandated to encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice (section 13, 1988 Act); and is obliged to prepare an annual report in relation to his activities under the Act and cause copies of this report to be laid before each House of Parliament (section 14, 1988 Act). [The Data Protection (Amendment) Act 2003 updated the 1998 Act, implementing the provisions of EU Directive 98/46.]

Under section 9 of the Communications (Retention of Data) Act 2011, the Garda Síochána (Irish police force), the Permanent Defence Forces and the Revenue Commissioners are obliged to submit reports in respect of data that were the subject of all disclosure requests made during the relevant 12 month period. The Minister for Justice, Equality and Law Reform is mandated to review reports submitted by the Garda Commissioner. The Minister for Defence is mandated to review reports submitted by the Chief of Staff of the Permanent Defence Forces and the Minister for Finance to review reports submitted by the Revenue Commissioners – before forwarding the reports to the Minister for Justice, Equality and Law Reform, along with any comments he or she may have. On receipt of all reports, the Minister for Justice, Equality and Law Reform is mandated to prepare a State report for submission to the European Commission.

Under sections 10 and 12 of the transposing legislation, the Complaints Referee and the designated High Court judge, who is to keep the operation of the legislation under review and ascertain if the Garda Síochána, Permanent Defence Forces and the Revenue Commissioners are complying with its provisions, are empowered to make reports to the Department of An Taoiseach (Irish Prime Minister).

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

No. There are no lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof.

The case taken by Digital Rights Ireland (see answer to question 2 above), which has led to a referral to the European Court of Justice, concerns the validity of the Directive itself (including in relation to the Charter of Fundamental Rights and the European Convention on Human Rights) and the validity of the data retention process in Ireland under Part 7 of the Criminal Justice (Terrorist Offences) Act 2005 (its compatibility with articles of the Irish Constitution and Articles 6(1), 8 and 10 of the ECHR). [Part 7 of the 2005 Act has been repealed by section 13 of the 2011 Act.]

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

N/A

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

N/A

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

N/A

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

Yes.

Case C-301/06: Ireland v. European Parliament and Council of the European Union, delivered on the 10th February 2009 [concluded].

Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources & Ors [2010] IEHC 221 [see further Part II of this report].

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

The transposing legislation contains no information in relation to the location at which the data are stored. The location at which the data are stored is the responsibility of the service providers.[3]

It has been reported that discussions on issues of this kind have been going on for some time between the service providers and the Department of Justice. Reports stated that a first draft of an agreement between them was leaked in September 2009 (see Karlin Lillington, 'Data Retention - Should it be left to a private agreement between the State and Telcos', The Irish Times, 25 September 2009). More recently a second draft has been leaked (see Digital Rights Ireland website, 'Data retention agreement between Department of Justice and telcos leaked', 20 September 2010).

[Update August 2013: A Memorandum of Undertanding (MoU) was signed by the representatives of the communications industry[4] and the relevant State agencies (Garda Síochána, Permanent Defence Forces and Revenue Commissioners) on 4th May 2011. The final version of the MoU is available on the website of the Internet Service Providers Association of Ireland (ISPAI) at http://www.ispai.ie/docs/MoUFinal-14Apr11.pdf.]

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

No such detail is included in the 2011 Act.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

Section 4(1) of the 2011 Act provides that retained data shall be subject to:

---

3 The authors received email correspondence to this effect from the Office of the Data Protection Commissioner on 11th October 2010.

4 For the purposes of the MoU, the "communications industry" consists of: (1) the Alternative Operators in the Communications Market (ALTO), which represents national and international operators in the fixed, wireless, mobile and cable sectors; (2) the Telecommunications and Internet Federation (TIF), which represents leading industry and associated interest groups in the field of electronic communications; and (3) the Internet Service Providers Association of Ireland (ISPAI), which represents the Irish ISP industry.

(aa) "appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; and
(bb) "appropriate technical and organisational measures to ensure that they can be accessed by authorised personnel only

The 2011 Act does not specify what would constitute "appropriate" measures. Such measures are believed to be the subject of ongoing negotiations between State agencies and the communications industry.

During the course of parliamentary deliberations on the transposing legislation, concern was expressed about the adequacy of the oversight regime (202(6) Seanad Debates 398 (29 April 2010)). The Data Protection Commissioner has also expressed concerns in this regard (see, for example, Data Protection Commissioner, Annual Report 2009, p.33).

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

Section 5 of the 2011 Act prevents service providers accessing data except inter alia in accordance with a court order. As explained above, senior officers of the Garda Síochána, Permanent Defence Forces and Revenue Commissioners can request disclosure. The request must normally be in writing but in cases of "exceptional urgency" it can be made orally, but if that is the case, the oral request must be confirmed in writing within two working days (s.6(4) and 6(5)).

c) data are not used for purposes other than those they are permitted to be used?

Please see answer to (a) above

The Complaints Referee (s.10 of the 2011 Act) and the designated judge (s.12), as described above) have roles in relation to the operation of the provisions of the legislation in practice.

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

Please see answer to (a) above. No details are provided in the Act.

e) **data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?**

Please see answer to (a) above. No details are provided in the Act.

f) **the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?**

Please see answer to question 18.

g) **sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?**

Please see answer to question 53.

41. **Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?**

The Data Protection Commissioner has a supervisory function (s.4) – the Data Protection Commissioner is the national supervisory authority for the purpose of the Communications (Retention of Data) Act 2011.

The Complaints Referee has an investigative function (s.10) – a person who believes that a disclosure request has been made in respect of data that relates to that person can apply to the referee to investigate the matter. The Referee can investigate whether a disclosure request was made and, if so, whether proper procedures were followed. If the Referee concludes that an infringement of section 6 took place he may direct that the data in the possession of the Gardaí, Permanent Defence Force or Revenue Commissioners be destroyed and recommend the payment of compensation by the Minister for Justice, Equality and Law Reform.

The designated judge has both supervisory and investigative functions (s.12) – the designated judge is responsible for reviewing the operation of the legislation and reporting to the Taoiseach (Prime Minister) in this regard. In addition, the designated judge may investigate any disclosure request and review any documents related to that request.

The office of the Data Protection Commisisoner has a role in ensuring that data are safeguarded in practice. For example, he reported in 2003 (Data Protection Commissioner, Annual Report, p.4) that an inspection was carried out at Eircom (telephone provider) to review that access to telephone traffic data by law enforcement agencies was in line with the legislation then in force.

In his annual report for 2009, the Data Protection Commissioner stated:

"The Data Protection Acts contain provisions permitting law enforcement agencies to process personal data for investigation purposes, however the retention of data

collected by this system in respect of law abiding citizens also had to be considered and a balance as to its retention reached. In this regard, we agreed an Automatic Number Plate Recognition (ANPR) policy document with An Garda Síochána. The guidance contained in this document aims to ensure that those deploying and operating ANPR can do so effectively while also recognising and respecting the rights and privacy of individuals."

The Commissioner also referred positively to the Garda Síochána in his 2008 report (Data Protection Commissioner, Annual Report, pp. 30 & 44).

However, the staff of the Commissioner's office have also commented on the very large number of disclosure requests made by the Garda Síochána (see answer to question 10 above) and a leaked draft of a European Commission report suggests that the number of requests is in fact substantially higher than previously thought.

[Update August 2013: On 27th September 2011, the Government decided to designate these duties to Mr. Justice Iarfhlaith O'Neill, Judge of the High Court – see Iris Oifigiúil (Irish State Gazette) No. 79, 4 October 2011, p.1350]. See also updated answer to question 6 on second questionnaire.]

42. What technical (de facto and/or de iure) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?

There are no technical standards in relation to the retention and transmission of data specified in the transposing legislation. However, section 2C of the Data Protection Acts 1988-2003 applies in this context.[5]

Section 2C of the Data Protection Acts 1988-2003 states:

2C. Security Measures for Personal Data

2C.-(1) In determining appropriate security measures for the purposes of section 2(1)(d) of this Act, in particular (but without prejudice to the generality of that provision), where the processing involves the transmission of data over a network, a data controller

(a) may have regard to the state of technological development and the cost of implementing the measures, and

(b) shall ensure that the measures provide a level of security appropriate to -

(i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and

[5] The authors received email correspondence to this effect from the Office of the Data Protection Commissioner on 11th October 2010.

(ii) the nature of the data concerned.

(2) A data controller or data processor shall take all reasonable steps to ensure that –

(a) persons employed by him or her, and

(b) other persons at the place of work concerned, are aware of and comply with the relevant security measures aforesaid.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall -

(a) ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the data controller and the data processor and that the contract provides that the data processor carries out the processing only on and subject to the instructions of the data controller and that the data processor complies with obligations equivalent to those imposed on the data controller by section 2(1)(d) of this Act,

(b) ensure that the data processor provides sufficient guarantees in respect of the technical security measures, and organisational measures, governing the processing, and

(c) take reasonable steps to ensure compliance with those measures.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

Section 6 of the transposing legislation sets out the procedure for making a disclosure request in respect of retained data (see answer to question 29).

The second draft of a Memorandum of Understanding (MoU), currently being drawn up by the Department of Justice and the various Irish service providers (ISPs and telecoms), was leaked in September 2010. According to the leaked document, the parties to the MoU – accessing bodies and the retaining bodies – agree to establish an authorised single point of contact within their organisation to which all data disclosure requests and responses will be made. Parties to the MoU further agree that the preferred mode of communication in this context will be secure electronic communication. In this regard, accessing bodies and retaining bodies will provide unique, digitally signed and encrypted e-mail addresses. Where for technical or operational reasons communication by secure electronic communication is not possible, parties to the MoU agree to provide an alternative fax number or emergency telephone number. Parties to the MoU also agree to endeavour to develop standardised request and response formats – a standard electronic mail and paper form – however, there will be no obligation on parties to use that form.

[See update above, question 37]

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

The transposing legislation does not specify the procedure for cross-border requests for retained data. However, it can be assumed that traditional mutual assistance routes would be available.[6]

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

The Data Protection Commissioner has reported on occasion his satisfaction that these matters have become the subject of public debate (see, for example, Data Protection Commissioner, Annual Report 2002, p.3).

The media, particularly the print media, frequently report and comment on the issues. The Irish Times and journalist Karlin Lillington of that newspaper are prominent in bringing developments in relation to data retention to the attention of the public.

A number of websites and blogs, for example the website of Digital Rights Ireland and the blog of T.J. McIntyre of Digital Rights Ireland, as well as those of a number of other organisations and individuals, such as practising and academic lawyers, constantly report and comment on developments with regard to data retention.

However, on 22 January 2008, McIntyre wrote in his blog:

"Yet so far there has been very little public debate. One reason might be that this surveillance happens invisibly in the background. But compared to traditional surveillance it is potentially far more intrusive, and carries much greater risks of abuse. In the United Kingdom we have seen the loss of data on many millions of individuals. Here officials in the Department of Social Welfare have been found to

[6] The authors received email correspondence to this effect from the Office of the Data Protection Commissioner on 11th October 2010.

be engaged in the systematic leaking and selling of personal information from government databases...

... Public awareness has also been stifled by the tactics adopted by the Government. In 2002 data retention was initially brought in by a secret ministerial order, which the telephone companies were forbidden to reveal. Only after pressure from the Data Protection Commissioner was it made public. In 2005, the Minister for Justice again avoided public scrutiny by changing the law using a last minute amendment to an unrelated Bill – breaking a promise that there would be full consultation and a separate Bill for the Oireachtas to debate." (www.tjmcintyre.com)

Two of Ireland's leading rights watchdogs, the Irish Council for Civil Liberties (ICCL) and Digital Rights Ireland joined calls from a network of European experts for an end to compulsory telecommunications data retention.

The ICCL also made a submission (November 2009) on how the 2009 Bill (now the 2011 Act) should be amended to protect fundamental rights. The ICCL drew attention to the blanket retention provided for in the 2009 Bill (now the 2011 Act) and recommended that data should be retained only where there is a legitimate suspicion that a serious offence has been committed. It also recommended retention periods of six months; that only Garda and Defence Forces personnel (not Revenue Commissioners) should be authorised to access communications data; that data requests should be subject to judicial approval; that comprehensive reporting mechanisms should be obligatory under the Bill as part of the independent judicial oversight framework; that statistical reports submitted for the relevant Ministers should be laid before the Houses of the Oireachtas and that appropriate remedies should be available under the Bill for individuals whose privacy was compromised by unauthorised or unfounded disclosure requests.

The Irish Human Rights Commission joined the Digital Rights Ireland High Court case as an amicus curiae.

The parliamentary debates contain contributions from the various political parties, but a consensus appears to have emerged that Sean Sherlock of the Labour Party was the most informed and had the most useful comments and proposals for amendment of the 2009 Bill (now the 2011 Act).

46. Are there any obligations in your country to retain other personal data without a specific reason (e.g. passenger name records (PNRs), employment data, etc)?

No. (No such obligations have been found in the course of the authors' research.)

However, it is worth noting that the Garda Siochána (Irish police force) uses Automatic Number Plate Recognition (ANPR) systems in its Garda Traffic Corps vehicles (http://www.garda.ie). This development has given rise to privacy concerns (see, for example, Digital Rights Ireland, 'Minister for Justice Ducks Questions on Number Plate Surveillance Scheme', 8th February 2006). The planned nationwide roll out of ANPR was completed in 2010.

The Data Commissioner agreed an APNR policy document with the Garda Síochána in this regard, which aims to ensure that those deploying and operating the APNR system can do so effectively while also recognising and respecting the rights and privacy of individuals (see Data Protection Commissioner, Annual Report 2009, p.27).

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

Section 9(5) of the transposing legislation provides that the reports to be submitted by the Garda Commissioner, Chief of Staff of the Permanent Defence Forces and Revenue Commissioners to the relevant Ministers shall include:

"(a) the number of times when data has been disclosed in response to a disclosure request,

(b) the number of times when a disclosure request could not be met,

(c) the average period of time between the date on which the retained data were first processed and the disclosure request."

During the course of parliamentary deliberations on the 2009 Bill (now the 2011 Act), it was proposed that these reports should also "contain details of the numbers of prosecutions actually commenced as a result of investigations to which requests related, and a detailed justification for any significant excess of numbers of requests over numbers of prosecutions actually commenced." (703(2) Dáil Debates 351 (24 February 2010)). This proposal was rejected on the grounds that the transposing legislation reflects exactly the requirements of Directive 2006/24/EC and to go beyond these requirements would "have no added value." (703(2) Dáil Debates 352 (24 February 2010)). In addition, it was argued that it "would be impossible to draw a direct correlation between requests submitted and prosecutions" given that access to data represents but one link in the evidentiary chain.

During the course of parliamentary deliberations on the transposing legislation, reference was made to two high profile murder cases during which "evidence intercepted by the Garda Síochána was critical in the conviction and incarceration of those guilty of serious crimes (202(6) Seanad Debates 399 (29 April 2010)). In both cases, access to the accused's mobile phone records played a key role in their conviction.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

No. The authors have not uncovered any such information during the course of research. However, the absence of such information is likely due to the fact that the

Communications (Retention of Data) Act 2011 has only been operational since 26th January 2011.

[Update August 2013: See updated answers to questions 6 and 14 on second questionnaire.]

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

It is clear, from the parliamentary deliberations relevant to the transposing legislation, that the periods of retention – 2 years in respect of telephony data and 1 year in respect of Internet data (the maximum retention periods permissible under Directive 2006/24/EC) – are proving controversial. Concern primarily centres around the financial burden which will be placed upon service providers by the legislative requirement to retain telephony data for this amount of time. (See further Q29) In addition, during the course of parliamentary deliberations, it was argued that retention periods of 2 years and 1 year were "excessive" and "against the European mainstream." (703(2) Dáil Debates 319 (24 February 2010)).

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[7] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

Privacy

The Irish Constitution of 1937, Articles 40 - 44 protect fundamental rights. Article 40 protects the personal rights of the citizen, including freedom of expression (Article 40.6.1), which is set out in detail. It also protects privacy as a personal right of the citizen (Article 40.3).

---

[7] In the following, "national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

The right to privacy is an unspecified right that has been recognised by the courts as being protected by the Constitution. For example, privacy in one's telephone conversations was recognised in 1987 in a case involving the tapping of two journalists' telephones: *Kennedy and Arnold v Ireland* [1987] I.R. 487. In that case the President of the High Court said that the tapping of their telephones was:

"[A] deliberate, conscious and unjustifiable interference by the State through its executive organ with the telephonic communications of the plaintiffs and such interference constitutes an infringement of the constitutional rights to privacy of the three plaintiffs."

In Digital Rights Ireland v the Minister for Communications & ors [2010] IEHC 222, the data retention challenge, Judge McKechnie stated in relation to the constitutional right to privacy (at paragraph 67 of the judgment):

"...such a right to privacy is not absolute. In particular, it may need to be balanced against the duty of the State to investigate and detect serious crime. Nonetheless, there has been much consideration of the status of evidence collected through such methods."

Judge McKechnie proceeded to cite Finlay C.J. in D.P.P. v. Kenny [1990] 2 I.R. 110 where he noted that:

> "[E]vidence obtained by invasion of the constitutional personal rights of a citizen must be excluded unless a court is satisfied that either the act constituting the breach of constitutional rights was committed unintentionally or accidentally, or is satisfied that there are extraordinary circumstances which justify the admission of the evidence in its (the court's) discretion."

McKechnie, J. went on to point out that (at paragraph 68):

"…it is clear that where surveillance is undertaken it must be justified and generally should be targeted."

<u>Confidential communication</u>

In *Digital Rights Ireland v the Minister for Communications & ors* [2010] IEHC 222, the judge proceeded to recognise a "general right to confidential communication" (para. 69, referring specifically to phone tapping and other communications interception, e.g. e-mail monitoring (para. 66).

The right to communicate is also protected by the Constitution as an unspecified right (Article 40.3), first identified by the courts in 1984.

In *Digital Rights Ireland*, the plaintiffs also claimed the corollary right to the right to communicate, i.e. the right to privileged communication (see para. 52 of the court judgment).

<u>Freedom of expression and of the press</u>

Freedom of expression is a specified right in the Irish Constitution (Article 40.6.1i). All citizens (including legal persons) have a right to express freely their convictions and opinions. The press, as organs of public opinion are also specifically mentioned in the freedom of expression article and their "rightful liberty of expression" recognised.

Freedom of conscience and freedom of religion

Both of these freedoms are guaranteed by the Irish Constitution (Article 44):

"Freedom of conscience and the free profession and practice of religion are ... guaranteed to every citizen."

The right to a fair trial

The right to due process is enshrined in Article 38 of the Constitution. (Articles 34-38 deal with the courts, the principle of open justice, the independence of the judiciary, etc.).

Other rights relevant to data retention

In the *Digital Rights* case, the plaintiffs claimed that the retention of digital data also infringed the right to family life (Article 41 of the Constitution) and the right to travel, and the attendant right to travel confidentially (unspecified rights protected by Article 40.3 of the Irish Constitution).

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The Constitution sets out the rights to be guaranteed and in some instances stipulates that they are subject to certain limitations. For example, freedom of expression is subject to public order and morality; freedom of the press must not be used to undermine public order or morality or the authority of the State. In addition, there is a clause in the freedom of expression section, which states that the publication or utterance of blasphemous, seditious or indecent matter is an offence which shall be punishable in accordance with law.

Thus, the permissible limitations on freedom of expression must be set out in statute or in common law. Statute law dealing with censorship of publications, film classification, defamation, etc., provide for the limitations on the constitutional right to freedom of expression.

As some of the rights mentioned above (e.g. the right to privacy and the right to communicate) are unspecified rights, the courts have to determine the scope of the rights and of the limitations in accordance with the spirit and ethos of the Constitution.

A Privacy Bill was published by the Government in 2006 but it was controversial on the grounds of its intrusion on freedom of expression and freedom of the press and the Government has not progressed it. Data Protection legislation (Data Protection Acts 1988-2003) protects privacy in personal communications.

It should be noted that the European Convention on Human Rights was incorporated into Irish law in 2003 (The European Convention on Human Rights Act 2003). As a result, the jurisprudence of the European Court of Human Rights can now be argued directly in Irish courts and Irish courts are obliged to have regard to that jurisprudence and, consequently, the limitations on the rights as set out in the ECHR and applied by the European Court of Human Rights.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

In *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources & Ors* [2010] IEHC 221, the High Court granted the Plaintiff's request that Directive 2006/24/EC be referred to the European Court of Justice (under Article 267 of the Treaty on the Functioning of the European Community (TFEU)) for a determination as to its validity.

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

As stated above (question 50), the Irish courts have established that a "deliberate, conscious and unjustifiable interference by the State through its executive organ with the telephonic communications" of citizens constitutes an infringement of the constitutional right to privacy.

Thus any such interference must be justified.

Additionally, in *Digital Rights Ireland v the Minister for Communications & ors* [2010] IEHC 222, Judge McKechnie in the High Court stated that the constitutional right to privacy "is not absolute. In particular, it may need to be balanced against the duty of the State to investigate and detect serious crime."

Therefore, the right to privacy is not absolute, it may be qualified, and a balancing of interests has to be undertaken by the courts.

While this statement was made in the context of the right to privacy, the balancing exercise to which the court refers applies equally to other qualified rights, forexample, the right to freedom of expression.

However, the judge in Digital Rights Ireland then cited an earlier case (see above Q.50) to the effect that the presumption would be against admitting evidence

obtained in breach of constitutional rights, unless the court was satisfied that: "either the act constituting the breach of constitutional rights was committed unintentionally or accidentally, or is satisfied that there are extraordinary circumstances which justify the admission of the evidence in its (the court's) discretion."

Therefore, where there has been a breach of constitutional rights in a situation of intentional, deliberate actions by the State, such as data retention, only extraordinary circumstances could justify admission of the evidence obtained. There have, however been a number of high profile murder trials, for example, where mobile telephone data have been admitted in evidence.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

The Data Protection Acts (1988-2003) provide in relation to sensitive personal data that:

2B (1) Sensitive personal data shall not be processed by a data controller unless

(a) section 2 and 2A (as amended and inserted, respectively, by the Act of 2003) are complied with [i.e. the conditions pertaining to the processing of personal data], and

(b) in addition, at least one of the following conditions is met:

(i) the consent referred to in paragraph (a) of subsection (1) of section 2A (as inserted by the Act of 2003) of this Act is explicitly given,

(ii) the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment,

(iii) the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where –

(I) consent to the processing cannot be given by or on behalf of the data subject in accordance with section 2A (1) (a) (inserted by the Act of 2003) of this Act, or

(II) the data controller cannot reasonably be expected to obtain such consent, or theprocessing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld,

(iv) the processing -

(I) is carried out in the course of its legitimate activities by any body corporate, or unincorporated body of persons, that –

(A) is not established, and whose activities are not carried on, for profit, and

(B) exists for political, philosophical, religious or trade-union purposes,

(II) is carried out with appropriate safeguards for the fundamental rights and freedoms of data subjects,

(III) relates only to individuals who either are members of the body or have regular contact with it in connection with its purposes, and

(IV) does not involve disclosure of the data to a third party without the consent of the data subjects,

(v) the information contained in the data has been made public as result of steps deliberately taken by the data subject,

(vi) the processing is necessary –

(1) for the administration of justice,

(11) for the performance of a function conferred on a person by or under an enactment, or

(111) for the performance of a function of the Government or a Minister of the Government,

(vii) the processing –

(I) is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or

(II) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

(viii) the processing is necessary for medical purposes and is undertaken by –

(I) a health professional, or

(II) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health professional,

(ix) the processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act, 1993, only for statistical, compilation and analysis purposes,

(x) the processing is carried out by political parties, or candidates for election to, or holders of, elective political office in the course of electoral activities for the purpose of compiling data on people's political opinions and complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects

(xi) the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest,

(xii) the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy or other moneys owed or payable to the State and the data has been provided by the data subject solely for that purpose,

(xiii) the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration of any benefit, pension, assistance, allowance, supplement or payment under the Social Welfare (Consolidation) Act 1993, or any non-statutory scheme administered by the Minister for Social, Community and Family Affairs."

In a related context, in *EMI Records (Ireland) Ltd and others v Eircom Ltd* [2010] IEHC 108, an agreement was reached by the parties to implement a "three strike rule." The Data Protection Commissioner was concerned that the operation of software to identify file sharers and the parties intention to collect, share and process IP addresses would constitute "personal data" and/or "sensitive personal data" (in that the data related to the commission of a criminal offence).

The judge decided, however, that the data involved did not constitute "personal data" under the Acts as the settlement did not involve the identification of any infringer and its entire purpose was to uphold the law. In relation to sensitive personal data, the judge found that there was nothing in the settlement or protocol agreed by the parties to suggest that anyone was being accused of a criminal offence and there was no issue beyond civil copyright infringement.

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

Digital Rights Ireland argued in the High Court that the Directive was contrary to Article 8 and Article 10 of the ECHR. Media reports indicate that the referral to the ECJ will be based primarily on Article 8 (privacy).

The question of the rights of companies was addressed in the Digital Rights Ireland case. Some personal rights are clearly inapplicable to companies, the Court said, but

property rights under the Constitution are capable of being enjoyed by corporate bodies (at para. 51 of the judgment).

In relation to the right to privacy, the Irish courts have not ruled out a right to privacy in business transactions, although it can only exist "at the outer reaches of and the furthest remove from the core personal right to privacy" (para.54). The judgment cites an academic work (O'Neill, The Constitutional Rights of Companies, 2007) in this regard to the effect that in the Irish constitutional context the right to privacy is concerned with securing individual autonomy and such autonomy considerations could not apply to a company. Nonetheless the judge took the view that a right of privacy in business transactions did exist although it would be of narrower scope. As companies are legal entities and an integral part of modern day business, he said, it is paramount that their interests are protected in the courts (para.56). He continued:

"...access may be sought to confidential information or research, or to information or documents generated as part of delicate business negotiations. Commerce and industry could not survive if such access was unregulated. It is therefore clear to me that in principle some right to privacy must exist at least over some areas of a company's activity." (para.56)

The judge further held that a person has a right not to be unjustifiably surveilled; that is, a general right to confidential communication, and that right would apply to corporate persons also (para. 69).

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

As indicated above, under the 2011 Act [the transposing legislation], only senior officers above a certain rank of the Garda Síochána, Permanent Defence Forces and Revenue Commissioners can request disclosure.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

As indicated above, there is no provision for costs in the 2011 Act. The issue of costs, although raised in submissions on the Bill by the Data Protection Commissioner and others, was not addressed in the Digital Rights Ireland case.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

The European Convention on Human Rights was incorporated (using the interpretative technique as in the UK Human Rights Act 1998) into Irish law by

statute in 2003 at sub-constitutional level. Therefore, the Irish Constitution takes priority in the case of conflict. The ECHR can be argued in the Irish courts and a declaration of incompatibility can be made by the courts. The Taoiseach (Prime Minister) is under an obligation to notify the parliament within 21 days of a declaration being made. It is then up to the Parliament whether to amend the legislation.

The status of the ECHR is therefore higher than that of other international laws that have been ratified but not incorporated into Irish law, except for EU law which has a special status under Article 29 of the Constitution.

The European Convention on Human Rights Act (ECHR) 2003 Act is intended to give further effect to the convention in Irish law. Section 2(1) of the ECHR Act provides:

"In interpreting and applying any statutory provision or rule of law, a court shall, in so far as possible, subject to the rules of law relating to such interpretation and application, do so in a manner compatible with the State's obligations under the Convention provisions."

In addition, section 3(1) of the ECHR Act 2003 provides that "subject to any statutory provision or rule of law, every organ of the State shall perform its function in a manner compatible with the State's obligations under the Convention provisions".

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

Article 29 of the Constitution deals with international relations and authorises the State to become a member of the EU and to ratify the relevant treaties. Article 29.4.7 further provides that:

"No provision of this Constitution invalidates laws enacted, acts done or measures adopted by the State which are necessitated by the obligations of membership of the European Union or of the Communities, or prevents laws enacted, acts done or measures adopted by the European Union or the Communities or the Institutions thereof, or by bodies competent under the Treaties establishing the Communities, from having the force of law in the State."

In 2006, the Department of An Taoiseach (Prime Minister) issued guidelines on best practice on transposition of EU directives

(Department of An Taoiseach, Guidelines on best practice on Transposition of EU Directives available at http://www.taoiseach.gov.ie/eng/Publications/Publications_Archive/Publications_2006/Final_Version_Guidelines1.rtf)

In short, following completion of negotiations/scrutiny and on receipt of a new Directive, the EU co-ordinator in the Department to whom the Directive has been assigned should inform the Department of An Taoiseach, the Department of Enterprise, Trade and Employment and the Department of Foreign Affairs, giving the name of the lead officer with responsibility for the transposition and the deadline for completion.

Preparation for drafting of legislation should start before or as soon as the Directive is published in the official journal of the EU. Consideration as to whether implementation/transposition should be by way of primary legislation or ministerial regulations (either pursuant to the European Communities Act 1972 or by other primary legislation which contains a specific power to implement/transpose EU legislation by regulations made under it) or through other alternatives to regulation, should be identified by the Regulatory Impact Assessment (RIA). RIA is a tool used for the structured exploration of different options to address particular policy issues. It is used where one or more of these options is new regulation or a regulatory change and facilitates the active consideration of alternatives to regulation or lighter forms of regulation.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

As explained above in answer to question 59, EU law has a special status in Article 29 of the Irish Constitution. Specific treaties of the Union from the setting up of the Community and Ireland's membership of it are referred to in Article 29.

However, the binding effect of a treaty depends upon ratification in accordance with Irish "constitutional requirements". As a result of a challenge to the way the Government approached the issue, a Supreme Court decision (Crotty v An Taoiseach [1987] IESC 4; [1987] IR 713 (9th April, 1987), in relation to the single European Act, decided that a referendum is required before a new Treaty can become law in Ireland.

In his judgment, the then Chief Justice stated (para. 62):

"The freedom to formulate foreign policy is just as much a mark of sovereignty as the freedom to form economic policy and the freedom to legislate. The latter two have now been curtailed by the consent of the people to the amendment of the Constitution which is contained in Article 29, s. 4, sub-s. 3 of the Constitution. If it is now desired to qualify, curtail or inhibit the existing sovereign power to formulate and to pursue such foreign policies as from time to time to the Government may seem proper, it is not within the power of the Government itself to do so. The foreign policy organ of the State cannot, within the terms of the Constitution, agree to impose upon itself, the State or upon the people the contemplated restrictions upon freedom of action. To acquire the power to do so would, in my opinion, require a recourse to the people "whose right it is" in the words of Article 6 "...in final appeal, to decide all questions of national policy, according to the requirements

of the common good." In the last analysis it is the people themselves who are the guardians of the Constitution. In my view, the assent of the people is a necessary prerequisite to the ratification of so much of the Single European Act as consists of title III thereof. On these grounds I would allow this appeal."

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

Only the central authorities are involved. See also answer to question 41.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

There is no further information available at this point.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

The transposing legislation gives rise to concern on a number of grounds, for example the length of the proposed retention periods, the wide range of offences that can justify the garda síochána accessing the data and the fact that the Revenue Commissioners can also access it.

Among the issues that have proven problematic are those to do with: (1) costs – specifically, the financial burden which will be placed upon Irish service providers by the legislative requirement to retain telephony data for 2 years and Internet data for 1 year and the government's failure to provide for the reimbursement of costs to service providers and (2) lack of sufficient safeguards and oversight mechanisms – for example, the fact that an individual has no right to be notified where his or her data has been the subject of a disclosure request. (See above question 18).

The insertion of a provision stating that an individual whose data have been the subject of a disclosure request must be notified of such disclosure within a specified period of time would go some way towards improving the transposing legislation from a rights perspective. Indeed, it has been argued that the complaints mechanism contained in section 10 of the transposing legislation – through which a data subject whose data has been the subject of a disclosure request may apply to the Referee for an investigation – is meaningless, in light of the fact that there is no duty to notify or inform that data subject that his or her data has been the subject of a disclosure request in the first place. (see 202(6) Dáil Debates 406 (29 April 2010)).

Balancing the interests in the context of data retention (INVODAS)

Ireland

Marie McGonagle and Sharon McLaughlin

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

No. National constitutional law does not expressly provide for a right to communicate anonymously.

The right to communicate is not specified in the Constitution but has been recognised by the courts as one of the personal rights of the citizen included by inference in Article 40.3.2:

> The State shall, in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name, and property rights of every citizen.

The right to communicate is therefore a constitutional right to be developed and delimited by the High Court and, on appeal, the Supreme Court, which are designated by the Constitution (Article 34.3.2) as having jurisdiction in constitutional matters.

Please see further answer to question 49 on first questionnaire ('confidential communications').

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime

Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

Amendments

There are currently no proposed amendments to the Communications (Retention of Data) Act 2011, signed into law by the President on 26th January 2011.

Proposals for improvement

The proposals for improvement set out in the answer to question 63 on the first questionnaire are discussed in the public sphere. In April 2011, an article by journalist Karlin Lillington in *The Irish Times* newspaper discussed the concerns of the ISP industry in the wake of the introduction of the 2011 Act (Karlin Lillington, 'Taxing and woolly data retention laws will discourage new business', *The Irish Times,* 15th April 2011).

The ISP industry has expressed concern about the broad definition of "service provider" contained in the Act (see answer to question 23 on the first questionnaire). Specifically, it is maintained that the broad definition of "service provider" contained in section 1(1) of the 2011 Act encompasses not only telecoms companies and conventional ISPs but also operators of cyber-cafés and hotels/hostels that offer Internet access to customers. It is further maintained that people who run Internet discussion boards potentially come within the remit of the legislation, depending on how such individuals manage e-mail services for board members.

Since the coming into effect of the 2011 Act, the ISP industry has reiterated its concerns about the costs involved in storing, maintaining and managing data in such a way as to make it quickly accessible to law enforcement agencies upon request (see answers to questions 27 and 28 on first questionnaire). Specifically, the ISP industry fear that the software, hardware and employee costs involved in complying with the 2011 Act "could prove crippling to smaller service providers and cause hotels to question whether to offer internet access at all."

It is argued that the requirement to retain Internet data for a period of one year and telephony data for a period of two years places Ireland at a "competitive disadvantage in attracting many internet-centric companies at a time when foreign direct investment is important to the national economic recovery" (Karlin Lillington, 'Taxing and woolly data retention laws will discourage new business', *The Irish Times,* 15th April 2011). It is further maintained that the ambiguity of the 2011 Act creates an environment of uncertainty which is unlikely to lead to expansion of existing services or to attract new services.

Paul Durrant (General Manager of the Irish Internet Service Providers Association - ISPAI) states that, while telecommunications companies already retain call data for billing purposes, ISPs do not normally keep or store the type of data they are now legislatively obligated to manage and, as a result, the complexity involved in managing and processing data disclosure requests is a pressing concern for the ISP

industry. In addition, Mr. Durrant asserts that ISPs are uncertain about what exactly they are required to retain.

The 2011 Act has been criticised for being vague and uncertain both in terms of its scope and application.

On 31st May 2011, the Minister for Justice indicated that Ireland would shortly ratify the Council of Europe's Cybercrime Convention:

"To enable Ireland's ratification of this Convention, my Department is currently engaged in the preparation of a Criminal Justice (Cybercrime) Bill. The Bill will create a range of offences relating to information systems and data, including illegally accessing a system, interference with systems or data and illegal interception of data. Offences will also be created in relation to hacker tools used for the commission of these offences. It is intended to incorporate any legislative requirements arising from the new EU Directive on Attacks against Information Systems, which is currently being negotiated, into the Bill. Negotiations on the draft Directive are ongoing. Ireland fully supports this important EU initiative and I recently had the opportunity to discuss some of the issues in the draft directive with other Ministers at the Justice and Home Affairs Council meeting in Luxembourg." [See speech by Minister for Justice at opening of Cybercrime Centre for Training, Research and Education in Dublin on 31 May 2011 available at http://www.justice.ie/en/JELR/Pages/SP11000071]

[**Update August 2013**: However, according to the website of the Department of An Taoiseach (Prime Minister), it is not yet possible to indicate when publication of the Criminal Justice (Cybercrime) Bill will occur.]

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, S.I. 336 of 2011, which transpose the E-Privacy Directive 2009/136/EC, came into operation on 1 July 2011. The Regulations, which apply to telecommunications companies and Internet Service Providers (ISPs), and to any entity using such communications and electronic communications networks to communicate with customers, contain new requirements concerning compulsory notification of data breaches, user consent for the placing of cookies on electronic devices, the making of direct marketing phone calls and the sending of electronic marketing messages. The Regulations proivde for heavier penalties for service providers who fail to notify customers and the Data Protection Commissioner of every breach. The Commissioner can also, for the first time, prosecute companies for allowing a data breach and fines of up to €250,000 can be imposed on conviction on indictment. Responsibility for implementing the Regulations lies with the Office of the Data Commissioner, which has published a

Guidance Note on the Regulations. [See further the website of the Department of Communications, Energy and Natural Resources at www.dcenr.gov.ie and the website of the Data Protection Commissioner at www.dataprotection.ie]

In his annual report for 2010 the Data Commissioner reports on his publication of a data security breach Code of Practice. This was one of the recommendations of a Working Group set up by the previous Minister for Justice, Equality and Law Reform which also recommended a strengthening of our data protection laws to provide for penalties for serious breaches. The Code focuses on informing the people affected by security breaches so that they can take appropriate measures to protect themselves. It also encourages organisations to voluntarily report incidents to the Commissioner's Office. [See Data Protection Commissioner, Annual Report 2010, pp.13-15]

A total of 410 data security breach incidents were reported to the Office in 2010, a 350% increase on the number of reports (119) received in 2009.

This large increase in reporting is a consequence of the more exacting demands of the Code of Practice.

[**Update August 2013**: In the first full year of the 2011 Regulations being in effect, 60 data security breach notifications were received from telecoms and ISPs and two telecoms companies were prosecuted for failing to meet their legal obligation in this regard. See Data Protection Commissioner, Annual Report 2012, p.12].

[**Update August 2013**: A total of 1,167 data security breach incidents were reported to the Office in 2011, a 300% increase on the number reported on in 2010; and a total of 1,666 data security breach incidents were reported to the Office in 2012, again an increase in the numbers reported in previous years. See Data Protection Commissioner, Annual Report 2010, p.15; Annual Report 2011, pp.12-13; Annual Report 2012, p.12].

Data Protection Acts 1988-2003

Section 8 of the Data Protection Act 1988, as amended, provides for the disclosure of personal data by a data controller in certain specified circumstances. Among these, is disclosure "for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders […]" (Section 8(b)). However, section 8 of the Act does not impose an obligation on data controllers to comply with such a request.

The individual's right to privacy must be weighed against the need to investigate offences. The data controller must satisfy itself that the provisions of this section are met before deciding whether or not it will comply with such a request. A data controller may do this by, for example, satisfying itself that the law enforcement authority seeking disclosure is doing so in good faith and that such disclosure is actually necessary for the investigation of an offence.

In addition, section 8(e) provides for disclosure of personal data by data controllers when "required by or under any enactment or by a rule of law or order of a court." If a data controller is under a statutory obligation to disclose personal data, or is ordered to disclose such data by a court, this will take precedence over the prohibition on further processing (which includes disclosure of personal data to third parties) contained in section 2(1)(c) of the 1988 Data Protection Act, as amended.

[See the website of the Data Protection Commissioner at www.dataprotection.ie]

The Criminal Justice Act 2011

Section 19(1) of the Criminal Justice Act 2011 provides that:

"A person shall be guilty of an offence if he or she has information which he or she knows or believes might be of material assistance in—
(*a*) preventing the commission by any other person of a relevant offence, or
(*b*) securing the apprehension, prosecution or conviction of any other person for a relevant offence,
and fails without reasonable excuse to disclose that information as soon as it is practicable to do so to a member of the Garda Síochána."

Relevant offences are listed in Schedule 1 of the Act and include offences relating to banking, investment of funds and other financial activities; company law offences; money laundering and terrorist offences; theft and fraud offences; bribery and corruption offences; a consumer protection offence (participating in, establishing, operating or promoting pyramid promotional schemes); and criminal damage to property offences. In addition, section 3(2) of the Act gives the Minister for Justice and Equality the power to designate other offences falling within the above categories as "relevant offences" for the purpose of the Act. The term "person" is not defined in the Act.

In addition, section 15(1) of the Criminal Justice Act 2011 provides:

"For the purposes of the investigation of a relevant offence, a member of the Garda Síochána may apply to a judge of the District Court for an order under this section in relation to—
(*a*) the making available by a person of any particular documents or documents of a particular description, or
(*b*) the provision by a person of particular information by answering questions or making a statement containing the information,
or both."

Any person who fails or refuses, without reasonable excuse, to comply with an order made under section 15 shall be guilty of an offence (section 15(15)). In addition, section 22 of the Act deals with liability for offences by bodies corporate.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying**

commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as evidence in court?

In Irish law, there exists a privilege against self-incrimination in criminal cases. This means that an individual does not have to answer any question(s) before a court of law that would tend to incriminate him/her. However, if an accused decides to testify, or give evidence, then that right is waived and the accused must answer questions put to him/her by the prosecution, and cannot refuse to do so on the basis that the answers would incriminate him/her.

This privilege against self-incrimination is related to the right to silence. Both the right to silence and the associated privilege against self-incrimination are derived from the common law principle that an accused person is innocent until proven guilty (beyond reasonable doubt). In *O'Leary v. Attorney General* [1995] 1 I.R. 254, the Irish Supreme Court held that the right is not only derived from common law but is also derived from the Constitution of Ireland (Article 38 on the right to a fair trial in due course of law and Article 40 on personal rights).

The right to silence is not absolute and may be legitimately restricted by legislation. For example, the Criminal Justice Act 1984, as amended by Part 4 of the Criminal Justice Act 2007, provides that inferences can be drawn from an accused's silence in certain circumstances in any proceedings against him/her for an arrestable offence, which is one that can result in imprisonment for 5 years or more. Similarly, the Criminal Justice Act 2006, as amended by the Criminal Justice (Amendment) Act 2009, provides in relation to organised crime offences that inferences may be drawn as the result of the failure, in particular circumstances, to answer questions.

The privilege against self-incrimination is not absolute. The case of *In Re National Irish Bank* [1999] 3 I.R. 145 concerned the Companies Act 1990, section 10 of which stipulates that company officials are obliged to give certain information under investigation or face prosecution for an offence, and section 18 of which stipulates that information obtained under section 10 can be used as evidence in a criminal prosecution of the same individual. The court had to decide whether interviewees had a right to refuse to answer questions put to them by inspectors on grounds of possible self-incrimination, and, if not, whether answers or other evidence obtained from interviewees could be used against them in any subsequent criminal trial. The Supreme Court found that the powers given to inspectors under the legislation were clear, proportionate and "no greater than the public interest requires" and, resultantly, interviewees were not entitled to refuse to answer questions properly posed to them pursuant to the inspectors' powers under the Act. In relation to whether answers or other evidence obtained from interviewees could be used against them in any subsequent criminal trial, the Supreme Court agreed with the High Court that the right to a fair trial is not infringed at the questioning stage and, where the use of interviewees' answers infringes (or threatens to infringe) a constitutional right of the witness, that right can be then asserted and vindicated. The Supreme

Court also added that, in order to be admissible at a criminal trial, a confession must be voluntary.

There is no difficulty in presenting data to an individual when they are in the witness box provided that this data was obtained legally, for example, as part of a criminal investigation, legitimate surveillance, etc. In relation to the Communications (Retention of Data) Act 2011, there would be no difficulty in presenting in court Internet and/or telephony data that had been legally retained and accessed under the Act. Prior to the 2011 Act, telephone data obtained by the Gardaí (police) from a mobile phone operator played a key role in a murder trial in 2007 (*DPP v O'Reilly* [2007] IECCA 118).

The privilege against self-incrimination is related to the right to silence insofar as an individual does not have to provide testimonial evidence that would be likely to incriminate him/her.

In cases in which they are not the accused/plaintiff/defendant, doctors, lawyers and other professionals cannot refuse to testify – if they did, they would be subpoenaed and obliged to furnish otherwise confidential information. A refusal to do so could amount to contempt of court, which is punishable by fines and/or imprisonment, unless the testimony involved breaching confidences within relationships (e.g. doctor/patient, priest/penitent, lawyer/client in relation to court proceedings), which attract a privilege recognised in law. This applies in both criminal and civil proceedings.

A claim of privilege may arise, e.g., legal professional privilege, public interest privilege, etc. If the information being requested fits into one of the grounds of privilege, the individual will not be required to divulge that information. However, the grounds of privilege are very specific.

In addition, in a criminal case, the Gardaí could obtain a search warrant to find and remove the required information.

5. Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?

The 2011 Act and the parliamentary deliberations surrounding this Act are silent on this issue.

The authors contacted the Criminal Law Reform Division of the Department of Justice on the 15th June 2011 regarding this operational aspect of the 2011 Act. The authors received a response on the 22nd June 2011 to the effect that the Criminal Law Reform Division does not have responsibility for this operational aspect of the 2011 Act. The Criminal Law Reform Division advised the authors that it had contacted the appropriate divisions within the Department of Justice and within the state bodies specified in the Act (Gardaí Síochána, Permanent Defence Forces and Revenue Commissioners) and it would revert to the authors once a response had

been received. To date [August 2011], the authors have not yet received further information.

[**Update August 2013**: A Memorandum of Undertanding (MoU), first and second drafts of which were leaked in September 2009 and in September 2010 respectively, was signed by the representatives of the communications industry[1] and the relevant State agencies (Garda Síochána, Permanenrt Defence Forces and Revenue Commissioners) on 4th May 2011. The final version of the MoU is available on the website of the Internet Service Providers Association of Ireland (ISPAI) at http://www.ispai.ie/docs/MoUFinal-14Apr11.pdf. See, in particular, Schedule 3 (Procedures for making and servicing a data request).]

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

No. There are no official statistics or other available information on the transmission of retained data to entitled bodies. The absence of such information is explained by the fact that the Communications (Retention of Data) Act 2011 was only recently signed into law (26th January 2011).

Figures for some particular categories of data for 2008, 2009 are provided in the Tables in the European Commission's Communication of April 2011 (COM (2011) 225 final Report, Brussels 18 April 2011.

[**Update August 2013**: Figures for 2010, released by the European Commission in 2012, show that there were 14,928 requests for retained data made by Irish authorities – the Gardaí, Permanent Defence Forces and Revenue Commissioners. Figures for 2011, released by the Department of Justice in July 2013, show that there were 12,675 requests for retained data made by Irish authorities. Of these 12,675 requests, 40% related to mobile phone activity. There were 4,105 instances of internet records being passed over, compared to 3,528 for landlines. [See Conor Ryan, 'State agencies target Irish phone and internet records', *The Irish Examiner*, 15 July 2013; see also Karlin Lillington, 'State agencies target Irish phone and internet records', *The Irish Times*, 25 July 2013.]

[1] For purposes of the MoU, the "communications industry" consists of: (1) the Alternative Operators in the Communications Market (ALTO), which represents national and international operators in the fixed, wireless, mobile and cable sectors; (2) the Telecommunications and Internet Federation (TIF), which represents leading industry and associated interest groups in the field of electronic communications; and (3) the Internet Service Providers Association of Ireland (ISPAI), which represents the Irish ISP industry.

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

It is difficult to say in vacuo, although the legislation has been widely criticised during its passage through the Oireachtas (National Parliament). The question of privacy and whether the safeguards are adequate may arise. However, it must be noted that any new legislation passed by the Oireachtas and signed into law by the President carries a presumption of constitutionality. If challenged in court, the presumption will only be rebutted if there is no possible interpretation of the provision(s) of the Act that is constitutional.

8. Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?

No. Only the content and interception of correspondence would be covered.

9. Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.

The impact of the proportionality test is difficult to assess in light of the fact that the courts tend to use the rhetoric of proportionality without much explanation (see, for example, the Supreme Court case of *Rev. Roy Murphy v IRTC* [1999] 1 I.R. 26).

The proportionality test was articulated in the case of *Heaney v. Ireland* [1994] 3 I.R. 593. In this case, the President of the High Court (Costello P.) stated that:

> "The objective of the impugned provision must be of sufficient importance to warrant overriding a constitutionally protected right. It must relate to concerns pressing and substantial in a free and democratic society. The means chosen must pass a proportionality test. They must:—
> (a) be rationally connected to the objective and not be arbitrary, unfair or based on irrational considerations;
> (b) impair the right as little as possible, and
> (c) be such that their effects on rights are proportional to the objective."

As was stated by the Supreme Court in *Re National Irish Bank* in 1999, the test of proportionality involves "asking whether the restriction which the impugned sections [of the legislation] place on the right to silence is any greater than necessary to enable the State to fulfil its constitutional obligations", for example in the context of an investigation into the Bank, "ensuring equality before the law and of protecting the property rights of every citizen."

Barrister and academic, Brian Foley, points out that the Irish courts' application of the proportionality test articulated in *Heaney* has been inconsistent and unexplained. Specifically, it is contended that in some cases the courts are "willing to allow the

legislature the balance of decision-making power over questions of the legitimacy of limiting constitutional rights." In other cases, however, the courts "will require the legislature only to follow [...] the least restrictive means possible in pursuing a legitimate legislative alternative." Foley argues that the court must clearly explain the choices it makes.

[Foley, Brian, "The Proportionality Test: Present Problems" [2008] *Judicial Studies Institute Journal* 67.]

In addition, the European Convention on Human Rights Act 2003 means that the ECHR approach to, and application of, the test of proportionality can be raised in Irish courts.

10. **Please provide an update on the current state of affairs of the case *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources & Ors* mentioned in your answer to the first questionnaire. Have the questions to be submitted to the ECJ been submitted in the meantime? Do you have any information on their wording, and on how the proceeding has evolved since the ruling of 5 May 2010?**

The authors emailed T.J. McIntyre of Digital Rights Ireland on 28th June 2011 regarding this question and received a response on 30th June 2011 to the effect that these questions had not yet been submitted as Digital Rights Ireland and the State were unable to agree a form of words for the questions. It was hoped that the matter would be listed before Justice McKechnie in the High Court before the end of the legal term (which ended on 29th July 2011).

On 27th January 2012, the Irish Human Rights Commission (IHRC), appearing as amicus curiae in the case, reported on the decision of the High Court to consult the Court of Justice of the European Union on the extent to which a national court is required by EU Treaties to inquire into and assess the compatibility of the implementing measures under an EU Directive with the EU Charter of Fundamental Rights in a case concerning the right to privacy. (See Irish Human Rights Commission (IHRC), *IHRC welcomes High Court decision to consult EU Court of Justice on Privacy Case*, 27th January 2012 available at http://www.ihrc.ie/newsevents/press/2012/01/27/ihrc-welcomes-high-court-decision-to-consult-eu-co/)

Dr Maurice Manning, President of the IHRC, stated:

"[…] the IHRC considers, as stated in our submission as amicus curiae to the High Court, that the Court of Justice of the European Union would give some guidance as to the relevance of the Charter of Fundamental Rights in cases such as Digital Rights, which involve important personal rights. The Charter is now the fundamental human rights instrument within the EU, but its impact has not yet been fully realised. The guidance now being sought by the High Court should give direction on this very fundamental point, making the human rights protections under EU law much more relevant to the individual. This will have significance in each State throughout the EU."

[**UPDATE July '13**: This case, which began in 2006 and was referred to the ECJ by the Irish High Court in 2012, was heard by the ECJ on 9th July 2013. See updated answer to question 2 on first questionnaire.]

11. Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.

There is no specific provision in the 2011 Act that prevents the same data from being retained more than once.

During the course of parliamentary deliberations on the 2011 Act, the need to ensure that data is retained in such a way as to avoid being retained more than once (in accordance with Recital 13 of Directive 2006/24/EC) was acknowledged. Specifically, it was stated that: "[...], if more than one service provider is in possession of particular data, only one need retain it for the purposes of the directive. The detail on which provider retains duplicated data can only be agreed in discussions between the service providers and the law enforcement authorities." (202(6) *Seanad Éireann* 409, 29 April 2010).

In addition, a Regulatory Impact Analysis (RIA) carried out by the Department of Justice in 2009 reiterated this point, stating that "[d]iscussions between the Garda Síochána and industry representatives will ensure an understanding of this point." (Department of Justice, Regulatory Impact Analysis on the Communications (Retention of Data) Bill 2009, 2009)

12. Do you have any news as regards the envisaged agreement between the service providers and the Department of Justice (see your answers e.g. to questions 33, 38, 43 of the first questionnaire)? If so, please provide details.

According to an article in Ireland's *IP and Technology Law Blog*, published in February 2011, the Memorandum of Understanding (MoU) between service providers and the Department of Justice has not yet come to fruition (Ireland's IP and Technology Law Blog, 11th February 2011). The authors could find no additional references to this MoU.

[**Update August 2013**: Please see updated answer to question 5 above.]

In particular: does this agreement include any further specifications regarding data security with respect to storage and transmission (objectives to be achieved – e.g. "adequate confidentiality" – and/or quality requirements to be fulfilled – e.g. an obligation to encrypt the data before transmitting them to the authorised bodies)? If so, please describe their content. Do they provide for measures in one or more of the following areas:

- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**

- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**
- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
- **access logging**
- **secure (irreversible) deletion after expiry**
- **error correction mechanisms (e.g. hash functions, checksums)**
- **secure data transmission (cryptographic security, postal delivery)**
- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**
- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**
- **staff training/internal control mechanisms to ensure compliance with the law and other rules**
- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

The authors cannot provide an answer to this question at this time as the agreement does not yet exist.

[**Update August 2013:** As stated in the updated answer to question 5 above, the final version of the MoU is available on the website of the Internet Service Providers Association of Ireland (ISPAI) at http://www.ispai.ie/docs/MoUFinal-14Apr11.pdf. See, in particular, Schedule 3 (Procedures for making and servicing a data request).

13. **Is the formal requirement of a referendum as a prerequisite to a conferral of national sovereignties to the EU in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?**

The authors are unaware of the existence of any such obligation in Irish law.

14. Please provide details to the following safeguards of the rule of law in detail:

requirement of a court order (question 17 of the first questionnaire): does the judgment in the *EMI v. Eircom* case, as referred to in your further comment to question 17 of the first questionnaire, mean that in a private law case directed against an unknown person, the court (and also the parties?) may obtain data retained under the 2011 Act for the purpose of litigation, although this is not provided for by the 2011 Act? If this is correct, on which law did the court base its judgment, and what further requirements (if applicable) have to be met in such a case for a court to order the disclosure of retained data?

The data may be obtained in criminal cases by the Gardaí (police), as set out in the 2011 Act. The *EMI v Eircom* case (2010) referred to above was decided on 16th April 2010. In a later case *EMI Records [Ireland] Ltd & Ors -v- UPC Communications Ireland Ltd* [2010] IEHC 377, decided on 11th October 2010, the same judge who had heard the earlier Eircom three strikes case referred to above, stated *inter alia*:

- "68. I find it impossible to recognise as a matter of constitutional law, that the protection of the entitlement to be left in the sphere of private communications could ever extend to conversations, emails, letters, phonecalls or any other communication designed to further a criminal enterprise. Criminals leave the private sphere when they infringe the rights of other, or conspire in that respect. ... In the case of internet file sharing to infringe copyright, I am of the view that there are no privacy or data protection implications to detecting unauthorised downloads of copyright material using peer-to-peer technology ... In this regard, I am taking into account the fact that the process of detection through DtecNet is essentially anonymous. As previously emphasised, a communication between the recording companies and an internet service provider, having used the facilities offered by the DtecNet, that in a particular month a certain one hundred subscribers downloaded an average of twenty copyright protected tracks each, illegally, giving a date and time and the IP address, discloses no information publicly. The recording companies do not thereby harvest the names and addresses of infringers of copyright for data purposes, or for future communication or for evidence in a potential criminal case. They get nothing apart from a set of numbers. As between UPC and their customers, any solution to this illegal activity is conducted privately as between them. They already know each other, as they are joined by a contract. That communication is within the range of matters over which an internet service provider is entitled to deal with its customer. The abuse of an internet service for copyright theft is a serious matter from the point of view of the general enforcement of copyright protection. An internet service provider is entitled to have a policy against it."

The judge noted also (at para.85) that copyright protection has been recognised by the courts as a right of private property and is therefore a right guaranteed by the Irish Constitution. He therefore considered in some detail the provisions of the Copyright Act 2000. He went on to reconsider his previous judgment:

"135. [...] In *EMI Records (Ireland) Limited v. Eircom Limited* [2010] IEHC 108, (Unreported, High Court, Charleton J., 16th April, 2010), as has been previously stated, a similar action had been brought against Eircom, as the largest internet service provider in the State. This was settled on the basis of a three strike policy that is fully set out in that judgment. That was a private matter between the parties as a matter of contract. The settlement was not authorised or ruled on by the Court. The Court had no function in that regard. The Court was, some months after the settlement, asked to determine the compatibility of aspects of that settlement with the Data Protection Acts 1988-2003, three issues having been raised in correspondence by the Data Protection Commissioner. In the light of the evidence in this case, and the conclusions that the Court has reached, the Court would wish to make it clear that this judgment is unaffected. I have reconsidered it in the light of the evidence and submissions in this case and I am of the view that the judgment is correct. [...]

Conclusion
138. Solutions are available to the problem of internet copyright piracy. It is not surprising that the legislative response laid down in our country in the Copyright and Related Rights Act 2000, at a time when this problem was not perceived to be as threatening to the creative and retail economy as it has become in 2010, has made no proper provision for the blocking, diverting or interrupting of internet communications intent on breaching copyright. In failing to provide legislative provisions for blocking, diverting and interrupting internet copyright theft, Ireland is not yet fully in compliance with its obligations under European law. Instead, the only relevant power that the courts are given is to require an internet hosting service to remove copyright material. Respecting, as it does, the doctrine of separation of powers and the rule of law, the Court cannot move to grant injunctive relief to the recording companies against internet piracy, even though that relief is merited on the facts."

- **sanctions in the case of infringements (question 30 of the first questionnaire): does the law provide for any criminal acts that shall be punished in the context of data retention, and/or do the injured persons dispose of any claim for damages, irrespective of (the outcome of) a Complaints Referee's investigation?**

  No. The Communications (Retention of Data) Act 2011 does not provide for any criminal acts that shall be punished in the context of data retention. During the course of parliamentary deliberations on the Act, it was suggested that "there should be sanctions for any breach of the procedures in the Act or any abuse of powers by individual members of any of the State law enforcement agencies in operating the data access provisions in the Act." (207(5) *Seanad Éireann* 297 (20 January 2011)). The then Minister of State at the Department of Foreign Affairs (Deputy Peter Power), who represented the Government at the Committee and Remaining Stages of the parliamentary deliberations on the legislation, responded:

"The Minister [the Minister for Justice] would prefer if the individual organisations used their existing disciplinary procedures once a matter is brought to light. […] The High Court judge will certainly have the power to bring a matter to light by publication to the Taoiseach or Minister for Justice and Law Reform. If any abuse of powers amounted to a criminal offence or a breach of one's constitutional rights, it would give rise to potential avenues to discipline the guilty party through civil or criminal law. The feeling is that discipline is best left to the disciplinary mechanisms within the individual organisations, provided there is a mechanism to convey the relevant information to the most senior persons in those organisations." (207(5) *Seanad Éireann* 298 (20 January 2011))

In relation to claims for damages, section 10(8) of the 2011 Act provides that: "A decision of the Referee under this section is final." The Act makes no further provision in respect of redress. Indeed, the making of a recommendation for payment of compensation to the applicant is at the discretion of the Complaints Referee (section 10(5)).

[**UPDATE July 2013**: Prior to the coming into effect of the 2011 Act, section 67 of the Criminal Justice (Terrorist Offences) Act 2005 – now repealed by the 2011 Act – provided for the appointment of a High Court judge to *inter alia* keep the operation of the provisions of this Part of the Act under review and ascertain whether the Garda Síochána and the Permanent Defence Force are complying with its provisions (the Revenue Commissioners were not an accessing body under the 2005 Act). Similarly, section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 – as amended by section 11 of the 2011 Act – provided for the appointment of a High Court judge to review the operation of the Act.

In his report for 2010, the designated judge stated that he had investigated a number of alleged breaches of section 64(2) of the 2005 Act and that these alleged breaches were now the subject of a criminal investigation. In addition, it was stated that the matter would be also be investigated by the Garda Síochána under the Garda Disciplinary Code. [See Mr Justice Iarfhlaith O'Neill, Report of the Designated Judge pursuant to section 8(2) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and section 71(1) of the Criminal Justice (Terrorist Offences) Act 2005 (2010)].

In August 2011, national media, reporting details of the case, detailed how a member of the Garda Síochána (Irish police force) had abused her position in the Crime and Security Branch to access the phone records of her ex-boyfriend. Following a Garda investigation, the Director of Public Prosecutions (DPP) directed that no criminal charges would be brought against the Garda. The Garda in question kept her job but was transferred to another Branch of the police force. [See John Mooney, 'Garda who spied on her boyfriend will keep job', *The Sunday Times*, 14 August 2011]. The lack of adequate and effective sanctions in this regard has been highlighted by the media [see, for example, Digital Civil

Rights in Europe (EDRI), 'No effective sanction for Police abuse of Irish data retention system', 24 August 2011]

15. **Do you have any news on your request to the Department of Justice as regards the remaining sub-questions of question 34 of the first questionnaire: do foreign state bodies avail dispose of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?**

Yes, the authors received a response from the Criminal Law Reform Division of the Department of Justice on 20th April 2011.

According to Recital 18 and Article 4 of Directive 2006/24/EC, Member States are required to ensure that data retained under the Directive are provided to competent national authorities in compliance with national legislation. Directive 2006/24/EC is silent on the issue of direct access to data by foreign state bodies and, accordingly, direct access to data by foreign state bodies is not provided for in the implementing legislation.

As already noted in the previous questionnaire, the ability to make a disclosure request is confined to three state bodies: the Garda Síochána; the Permanent Defence Forces; and the Revenue Commissioners (see section 6 of the 2011 Act). As already noted, the 2011 Act is silent on the issue of direct access to data by foreign state bodies and, therefore, does not stipulate which authority is responsible for receiving disclosure requests from foreign state bodies under the 2011 Act.

However, section 6(4) of the Criminal Justice (Mutual Assistance) Act 2008 provides that a request for assistance [under the mutual legal assistance in criminal matters framework] must be addressed to the Central Authority in the State (unless the relevant international instrument provides otherwise). Section 8(1) of the 2008 Act provides: "The Minister is the Central Authority for the purposes of this Act." Section 2(1) designates the Minister for Justice and Equality as the relevant government minister in this regard.

Under section 5 of the 2011 Act, data may be accessed on foot of a court order. It is possible that a court order could be the result of a request for evidence from a foreign state through the existing mutual legal assistance in criminal matters framework (Criminal Law Reform Division, Department of Justice, April 2011).

Mutual legal assistance means that any country may make a request to Ireland for assistance in criminal investigations or criminal proceedings and that Ireland may make a request to other countries for assistance. The relevant legislation is Part VII of the Criminal Justice (Mutual Assistance) Act 2008 (Department of Justice, Mutual Legal Assistance).

16. As regards your answer to question 35 of the first questionnaire:

I understand from your answer to my remark *m9* in the first questionnaire that the Data Protection Commissioner does not take any directions from another body, and that there is no supervisory control over their acts other than an obligation to report annually to the Parliament. Is this understanding correct?

Yes, this understanding is correct.

Which body (the Data Protection Commissioner, the High Court judge or another body) is in charge of monitoring compliance of the service providers with the data retention obligations, as far as these obligations do *not* refer to the protection of personal data (e.g. compliance with Art. 3 or 7 of the 2011 Act)? Is this body independent in the sense of what has been said in question 35 of the first questionnaire?

Both the Data Protection Commissioner and the designated High Court judge have obligations in this regard.

Under section 12(1) of the 2011 Act, one of the functions of the designated judge is to "keep the operation of the provisions of this Act under review."

In addition, the Data Protection Commissioner, under section 4(2) of the 2011 Act, is designated as the national supervisory authority for the purposes of the Act and Directive 2006/24/EC.

Is my understanding correct that the High Court judge and the Complaints Referee are the bodies responsible for supervising that the bodies entitled to obtain access to the data retained (police etc) act within the law? If so: what role does the High Court play in carrying out this task, as opposed to the Complaints Referee? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

Section 10 of the 2011 Act provides for an independent complaints procedure. Under section 10 of the 2011 Act, where a person believes that the data relating to him or her are in the possession of a service provider and have been accessed on foot of a disclosure request, that person may apply to the Complaints Referee for an investigation into the matter. As part of this process, the Complaints Referee will (among other things) investigate whether the accessing body, in making the disclosure request, complied with section 6 of the Act. It is important to note that the Complaints Referee will only investigate a disclosure request on foot of the receipt of a complaint.

This complaints procedure was criticised during the course of parliamentary deliberations on the implementing legislation. Specifically, it was argued that the provision was "meaningless as a means of securing redress because the legislation does not include a mechanism whereby a person whose data has been disclosed

would be informed or notified of such disclosure." (202(6) *Seanad Éireann* 406, 29 April 2010).

Under section 11 of the 2011 Act, the president of the High Court may invite a serving judge of the High Court to undertake the duties specified in section 12 of the Act.

Section 12(1) of the Act provides that the designated judge shall keep the operation of the provisions of this Act under review, ascertain whether the Garda Síochána, the Permanent Defence Force and the Revenue Commissioners are complying with its provisions, and report to the Taoiseach (Prime Minister) on such matters as he/she deems appropriate. The designated judge also has the power to investigate any case in which a disclosure request is made and may access and inspect any official documents or records relating to the request (Section 12(2)). The designated judge may also communicate with the Taoiseach or the Minister concerning disclosure requests and with the Data Protection Commissioner in connection with the Commissioner's functions under the Data Protection Acts 1988 and 2003 (section 12(4)).

Section 12 of the 2011 Act was also criticised during the course of parliamentary deliberations, with one parliamentarian stating that reports of the designated judge (under other legislation) tended to be "rather cursory, consisting of one line stating that legislative provisions have been complied with", and alluding to the need to ensure that, under section 12, more detail is provided in these reports. In addition, section 12 was criticised for failing to provide sanction(s) where there is found to be an abuse of process by the accessing body. (202(6) *Seanad Éireann* 405, 29 April 2010).

In essence, the role of the Complaints Referee is investigative, while the role of the High Court judge is supervisory.

[**Update August 2013**: see also updated answer to question 41 on first questionaire.]

17. Does the statute incorporating the ECHR prevail over other (sub-constitutional) national law in case of a conflict?

No. The ECHR Act 2003 does not prevail over other sub-constitutional national law in case of a conflict.

Section 2 of the ECHR Act 2003 provides:

"(1) In interpreting and applying any statutory provision or rule of law, a court shall, *in so far as is possible*, *subject to the rules of law relating to such interpretation and application*, do so in a manner compatible with the State's obligations under the Convention provisions." [Emphasis added]

The interpretative obligation contained in the 2003 Act is weak and has not yet been definitively explored.

18. As regards your further comment to question 59 of the first questionnaire: please explain what alternatives to regulation are considered when applying the RIA tool (e.g. self-regulatory or co-regulatory mechanisms etc)?

The Irish Government's '*Regulating Better: A Government White Paper setting out six principles of Better Regulation*' (Appendix 1 of which deals with RIA) acknowledges that "State regulation is not always the best option and alternatives to regulation, or different regulatory approaches, need to be examined. […] This includes the use of available instruments, whether singly or in combination, or the possibility of the State taking no action where the problem can be solved by other means."

The White Paper further states that: "Alternatives to traditional "command and control" type regulation/legislation will be promoted and developed for wider use by Government Departments and Offices. This could include new approaches to regulation, including *co-regulation* and *performance-based regulation* (where the overall goal is stated but maximum flexibility is permitted as to how the goal can be achieved)." [Emphasis added]

(Department of an Taoiseach, *Regulating Better: A Government White Paper setting out six principles of Better Regulation* available at http://www.betterregulation.ie)